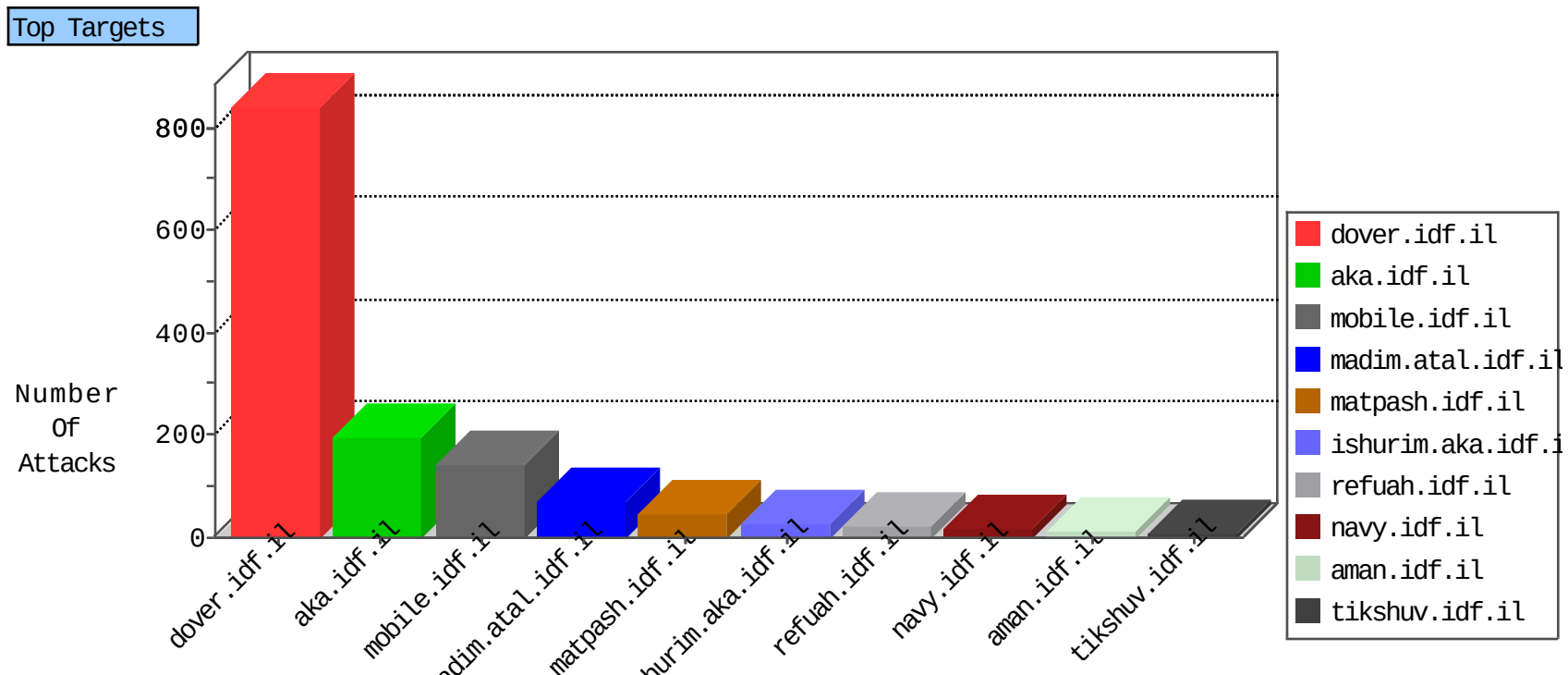
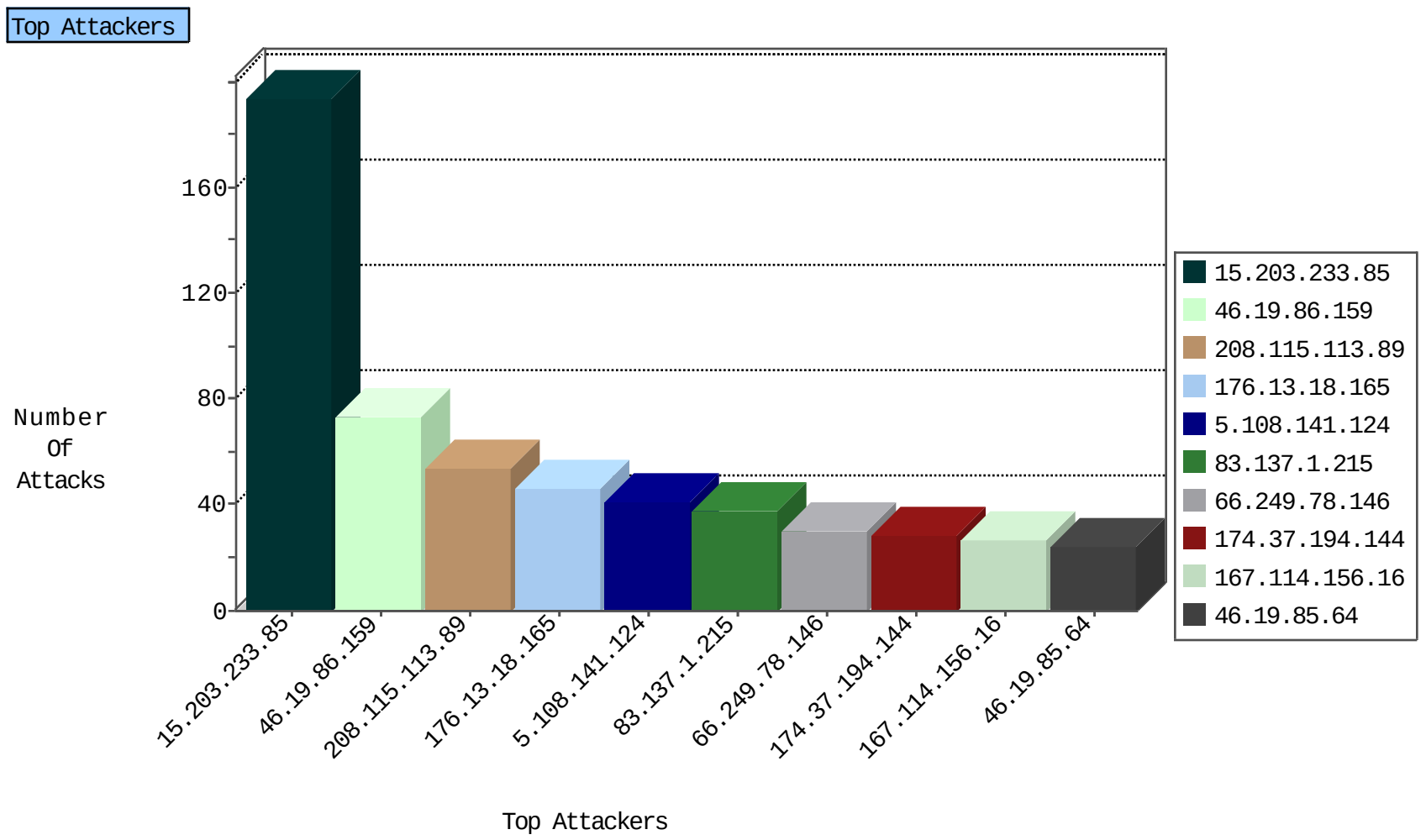
04-28-2016-09:04:07 to 04-28-2016-10:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-28-2016-09:04:07 to 04-28-2016-10:04:07

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	HTTP-POST-Segmented-DoS	dest-reset	989
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	485
80.74.96.29	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
183.60.48.25	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
172.82.142.122	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
5.206.231.84	Portugal	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
195.154.181.126	France	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
123.151.42.61	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
172.82.142.122	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
79.103.125.194	Greece	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
123.249.27.29	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
190.253.212.51	Colombia	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
94.102.49.116	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

04-28-2016-09:04:07 to 04-28-2016-10:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-28-2016-09:04:07 to 04-28-2016-10:04:07

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	3
13.92.84.22	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
219.127.49.142	147.237.76.42	Japan	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
200.195.135.82	147.237.8.14	Brazil	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
163.172.140.23	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
107.158.255.194	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
13.92.84.22	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
13.92.84.22	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
200.195.135.82	147.237.8.14	Brazil	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
200.195.135.82	147.237.8.14	Brazil	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
163.172.140.23	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
107.158.255.194	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
80.82.78.38	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1

04-28-2016-09:04:07 to 04-28-2016-10:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
15.203.233.85	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	194
46.19.86.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
5.108.141.124	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
83.137.1.215	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
36.69.220.158	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
37.231.84.201	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
185.120.125.15	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
176.13.16.255	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
80.246.137.127	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
88.254.109.108	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.98.155.80	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
217.128.133.161	France	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	11
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
69.31.51.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.46.13.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
87.203.102.200	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
128.242.249.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.179.195.7	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.43.104.156	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
46.43.104.156	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
213.244.82.139	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.66.13	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.244.82.139	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.64	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.149.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.190	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
82.80.57.18	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
66.249.93.182	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.125.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.64	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.0.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.57.18	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.71.107.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

04-28-2016-09:04:07 to 04-28-2016-10:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
46.19.86.159	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
213.57.40.25	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	8
37.46.39.112	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	8
79.178.84.17	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/searchresults/mobile	Block	7
46.19.85.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.13.16.255	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
93.172.207.19	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter RepeatPassword	Block	3
213.8.53.181	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	3
37.26.147.149	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	3
46.116.223.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.149.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
207.46.13.2	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.53.29.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.179.195.7	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
81.218.116.129	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/templates/general/mobile	Block	2
2.53.7.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.120.199.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
41.38.73.242	Egypt	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
84.109.10.105	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
71.6.146.185	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
46.19.86.45	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
108.84.188.130	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
5.102.195.108	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	1
87.71.19.120	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
80.74.103.200	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/giyus/www.navy.idf.il	Block	1
46.121.118.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
94.23.40.23	France	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 94.23.40.23	Block	1
41.38.73.242	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
87.69.30.207	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
79.176.72.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
109.186.16.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
87.71.19.120	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 1žÎÐ¸`ø'þQ[[#17]]mŠÚ²£º[[#7]]\[[#25]]©¯Ï,[[#30]][[#19]]\[[#6]]I"¹ß"³[[#6]]81¾ŒU[[#29]]æ•ðö'[[#6]]6PùÀÂ"yMP&äÇd†et>SØÖ[[#23]]•‰Z^Ž¡›¬e•–5Ä)ÇT}¶[[#5]][[#21]]¸[[#4]]ëÿá3g¼šsÒÙ¥ in URL	Block	1
80.246.133.38	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/57056.pdf&ved=0ahukewj88mpmt6fmahuc_iwkhwntar4qfggdmai&usg=afqjcnf1yolugsboijiblzxiye0gplabcg&sig2=sljt3vnb9hu32rwuqzye5w	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1607-15301-he/mmmmmmm=07f3c221mmmmmmm_07f3c221	Block	1
66.249.64.3	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
94.159.245.199	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/sachar	Block	1
87.71.19.120	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
79.178.84.17	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/mobile	Block	1
220.255.146.147	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
149.78.204.187	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
91.199.69.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter sbredirect in www.aka.idf.il/main/sachar/	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
108.84.188.130	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/mobile	Block	1
46.19.85.194	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
87.71.19.120	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method 1žÎÐ¸`ø'þQ[[#17]]mŠÚ²£º[[#7]]\[[#25]]©¯Ï,[[#30]][[#19]]\[[#6]]I"¹ß"³[[#6]]81¾ŒU[[#29]]æ•ðö'[[#6]]6PùÀÂ"yMP&äÇd†et>SØÖ[[#23]]•‰Z^Ž¡›¬e•–5Ä)ÇT}¶[[#5]][[#21]]¸[[#4]]ëÿá3g¼šsÒÙ¥	Block	1
46.117.27.42	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
157.55.39.106	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12535-he/dover.aspxמתג''סם	Block	1
93.172.154.44	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/67906.pdf	Block	1

04-28-2016-09:04:07 to 04-28-2016-10:04:07