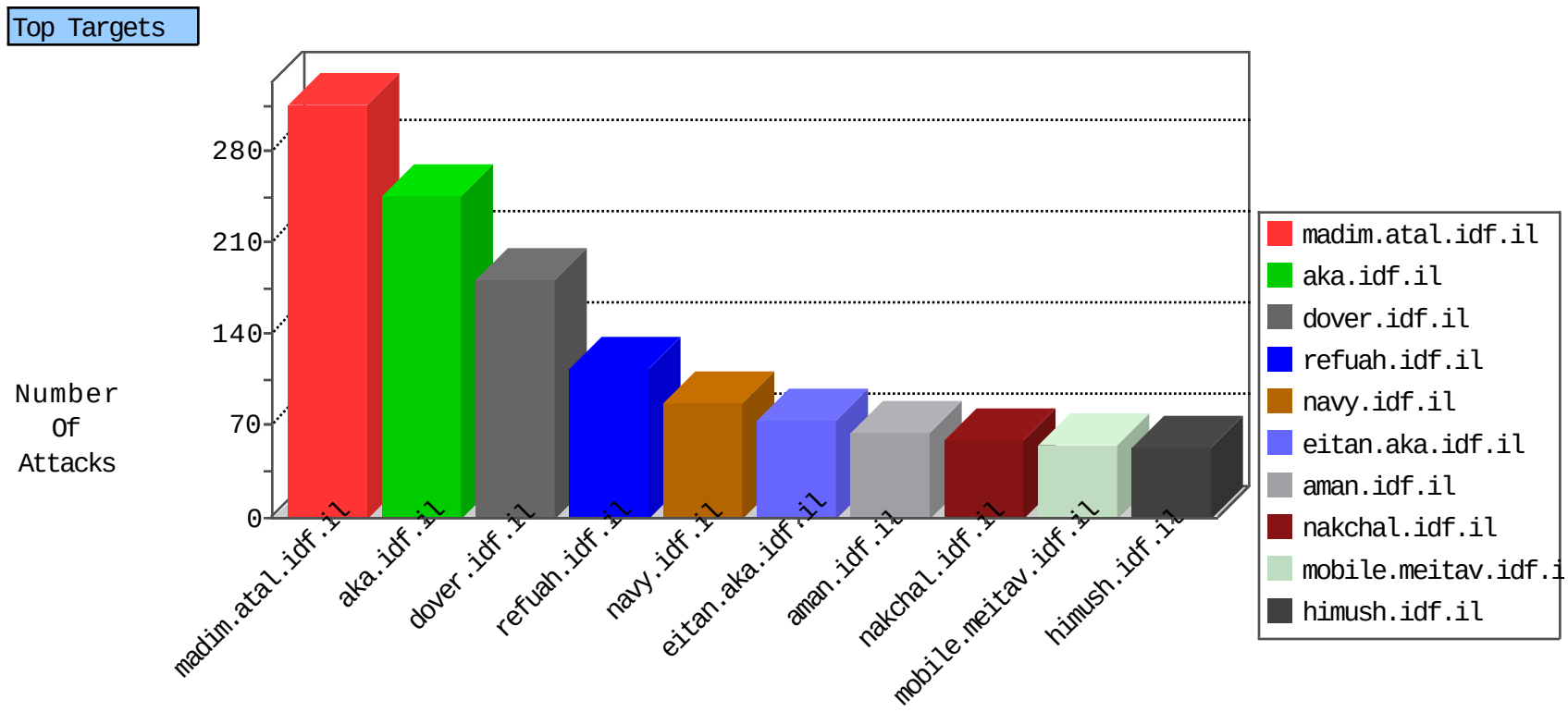
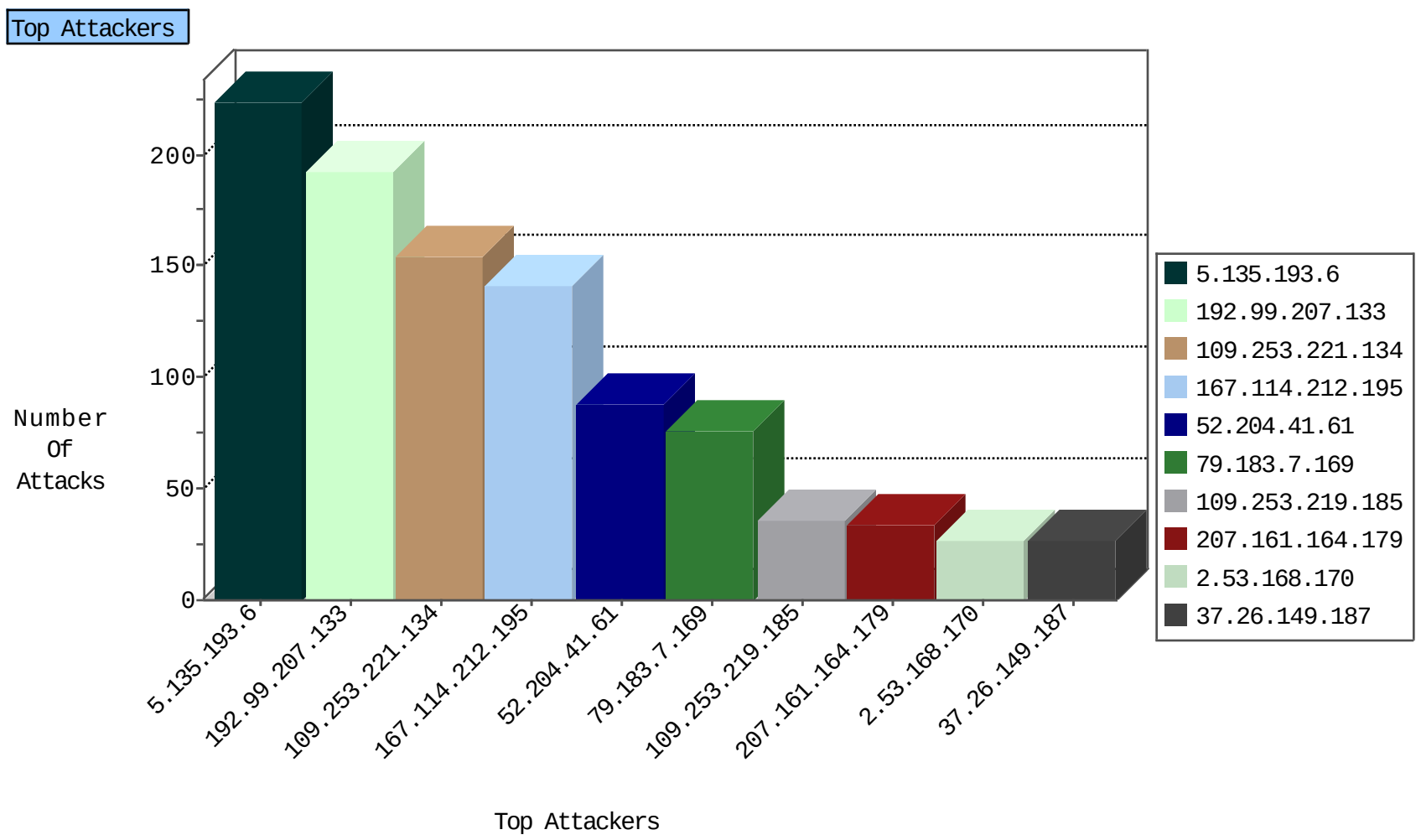
09-05-2016-20:04:00 to 09-05-2016-21:04:00

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-05-2016-20:04:00 to 09-05-2016-21:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-05-2016-20:04:00 to 09-05-2016-21:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.38.71	Germany	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	3
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
71.180.24.53	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-05-2016-20:04:00 to 09-05-2016-21:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
217.132.239.169	147.237.76.31	Israel	nakchal.idf.il	ET SCAN NMAP -sA (2)	5
39.47.61.53	147.237.77.216	Pakistan	dover.idf.il	ET WEB_SERVER Poison Null Byte	1
91.201.236.155	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
82.114.179.186	147.237.77.233	Yemen	atal.idf.il	ET SCAN NMAP -sS window 3072	1
45.79.95.64	147.237.72.166	United States	aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
185.93.185.10	147.237.72.167	Ukraine	ishurim.aka.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.114.179.186	147.237.77.233	Yemen	atal.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.86.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-05-2016-20:04:00 to 09-05-2016-21:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
192.99.207.133	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
192.99.207.133	Canada	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
192.99.207.133	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
192.99.207.133	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
192.99.207.133	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
192.99.207.133	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
192.99.207.133	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
192.99.207.133	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
82.145.211.207	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
167.114.212.195	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
167.114.212.195	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
167.114.212.195	Canada	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
167.114.212.195	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
167.114.212.195	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
167.114.212.195	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
109.65.38.142	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
167.114.212.195	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
167.114.212.195	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
2.55.20.247	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.116.105.172	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.121.244.225	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
5.135.193.6	France	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
5.135.193.6	France	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
5.135.193.6	France	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.86.141	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	11
2.53.168.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
5.135.193.6	France	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
207.161.164.179	Canada	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	10
5.135.193.6	France	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
5.135.193.6	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
5.135.193.6	France	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
5.135.193.6	France	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
5.135.193.6	France	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
5.135.193.6	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
5.135.193.6	France	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
5.135.193.6	France	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
37.26.149.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
5.135.193.6	France	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
2.53.168.170	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
37.26.149.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
207.161.164.179	Canada	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
5.135.193.6	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
5.135.193.6	France	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
37.26.149.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
109.75.78.69	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.135.193.6	France	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
5.135.193.6	France	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.86.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.135.193.6	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
5.135.193.6	France	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9

09-05-2016-20:04:00 to 09-05-2016-21:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.221.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	152
79.183.7.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
109.253.219.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
37.142.187.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
176.228.57.238	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.23.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
213.57.155.196	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
81.218.225.134	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
77.138.15.7	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	2
46.19.85.22	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
73.1.216.151	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
80.230.228.59	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
187.227.52.244	Mexico	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
77.124.12.206	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1
109.67.19.242	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.230.229.189	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
39.47.61.53	Pakistan	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
79.180.104.246	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1121-he/atal.aspx	Block	1
2.53.14.38	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
213.8.204.36	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.8.204.36	Block	1
66.249.69.14	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
84.229.10.56	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
45.79.95.64	United States	147.237.72.166	aka.idf.il	Malformed URL	Block	1
39.47.61.53	Pakistan	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
80.230.229.98	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
199.30.25.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.108	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
109.67.192.197	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.230.229.222	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
39.47.61.53	Pakistan	147.237.77.216	dover.idf.il	Malformed URL ≍Ÿcn″gƉqckÊ[[#15]]™@[[#2]]c`	Block	1
2.53.22.196	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.8.204.36	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
176.228.18.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.39	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding 82G0l3ebf[@G}u@oTlGh8I]nprO in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
85.64.129.113	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
45.79.95.64	United States	147.237.72.166	aka.idf.il	Unknown HTTP Request Method 1 in URL	Block	1
39.47.61.53	Pakistan	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name	Block	1
80.230.229.102	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.139.84.190	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
208.81.64.248	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
46.120.247.234	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
80.246.138.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
39.47.61.53	Pakistan	147.237.77.216	dover.idf.il	NULL Character in Method i[[#0]][[#0]][[#0]]v1@Ú–?W½[[#29]]ñ[[#0]]«¢ÄÄlÞì€l[[#25]]üÆ[[#7]][[#20]]égm¿^þ•êe^.[[#1]]ÑØ¦c¡}á_S€È‹.·1îík:	Block	1
80.230.228.54	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.210.186.57	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/0303-1.stm,	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21502-he/idfgdover.aspx	Block	1
86.200.225.160	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
39.47.61.53	Pakistan	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method i[[#0]][[#0]][[#0]]v1@Ú–?W½[[#29]]ñ[[#0]]«¢ÄÄlÞì€l[[#25]]üÆ[[#7]][[#20]]égm¿^þ•êe^.[[#1]]ÑØ¦c¡}á_S€È‹.·1îík:	Block	1
80.230.229.103	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

09-05-2016-20:04:00 to 09-05-2016-21:04:00