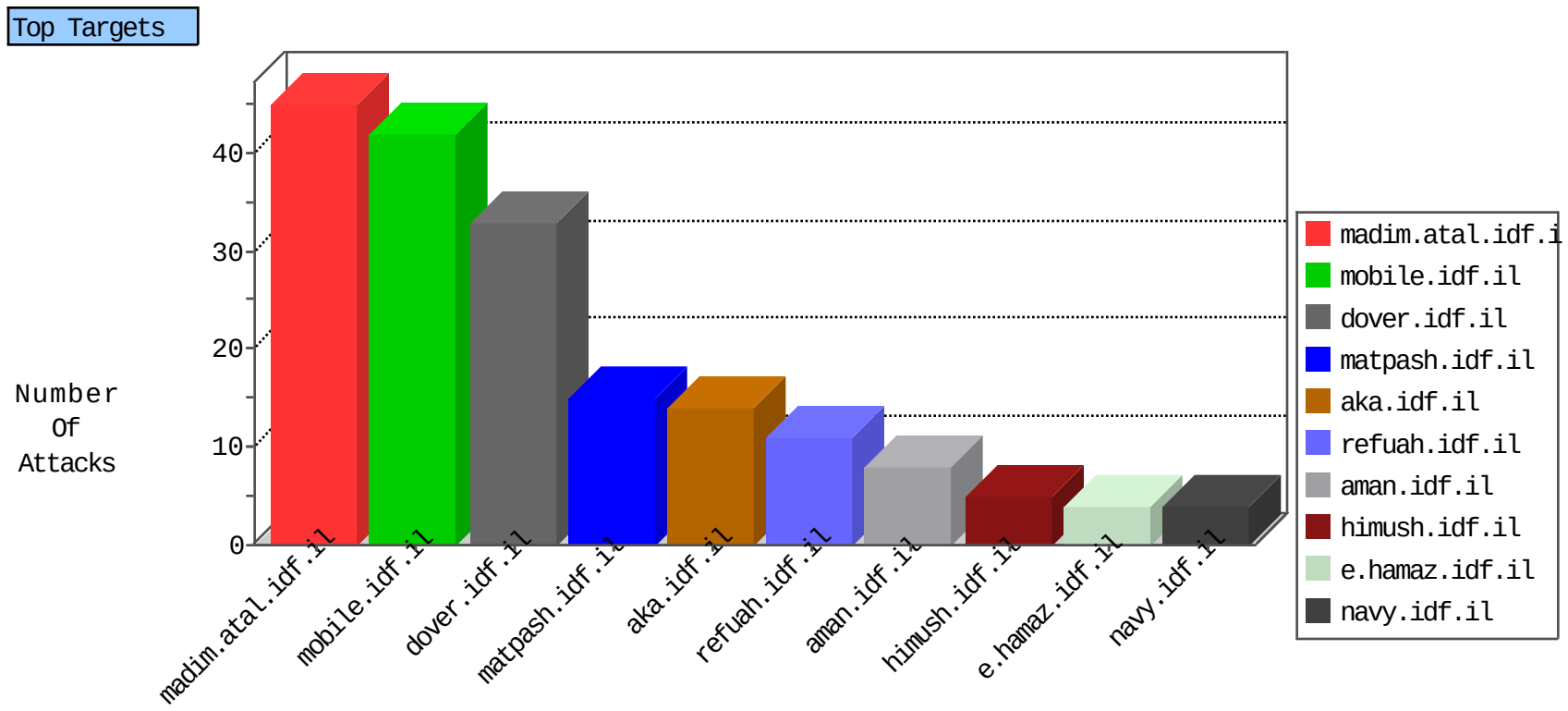
09-26-2016-06:04:09 to 09-26-2016-07:04:09

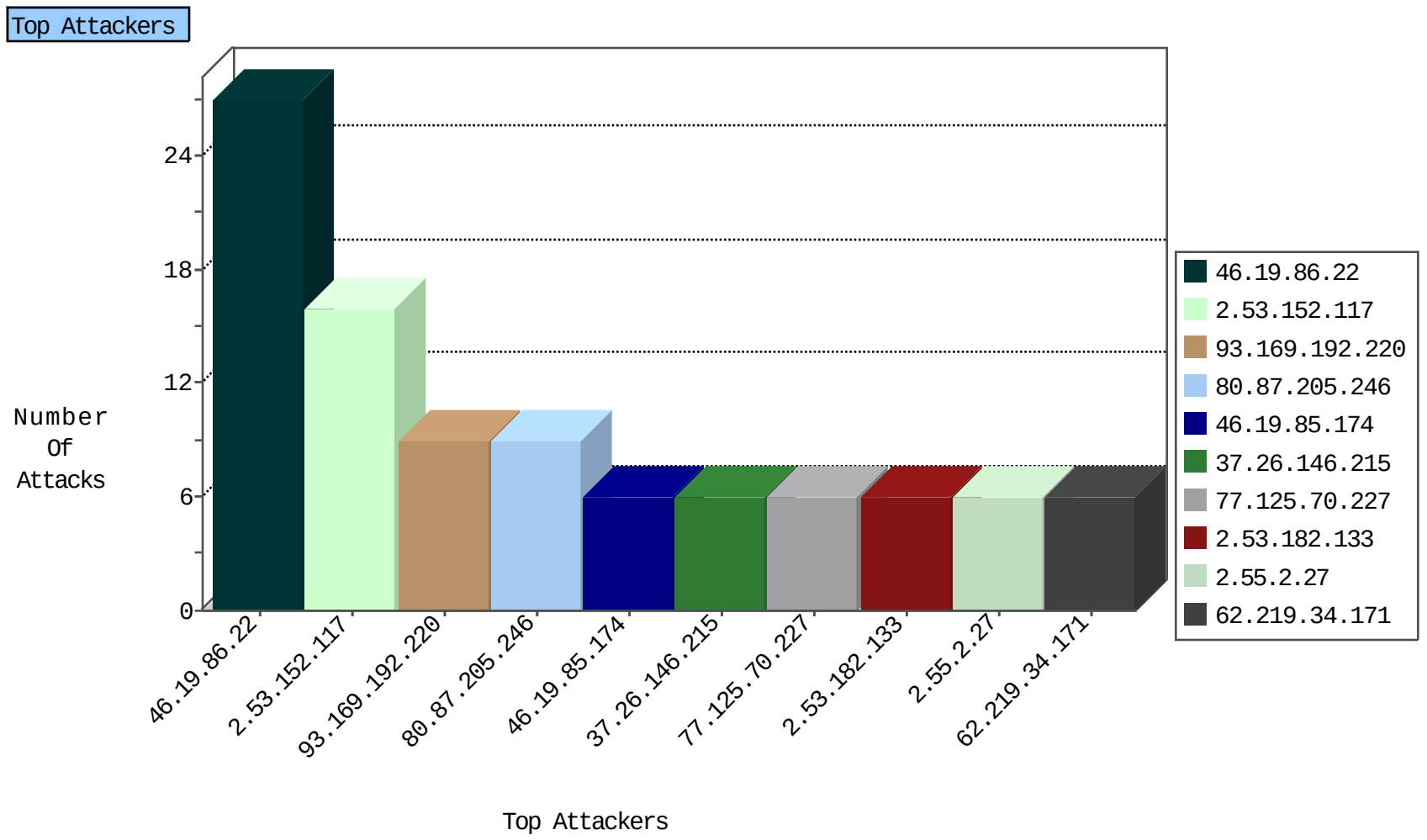
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-26-2016-06:04:09 to 09-26-2016-07:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
63.141.242.194	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
204.12.220.85	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
69.30.226.221	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
63.141.231.194	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
142.54.174.86	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
209.126.136.2	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
108.61.204.80	United States	147.237.76.34	yohalan.idf.il	Black List	drop	1
63.141.242.196	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
208.110.84.67	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
69.30.227.218	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
63.141.231.211	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
185.94.111.1	Russian Federation	147.237.76.176	test.ncore.idf.il	Black List	drop	1
63.141.242.198	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
208.110.84.69	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
93.158.200.96	Netherlands	147.237.76.201	e.atal.idf.il	Black List	drop	1
63.141.242.194	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
204.12.220.85	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
63.141.242.198	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1

09-26-2016-06:04:09 to 09-26-2016-07:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
36.110.147.96	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-26-2016-06:04:09 to 09-26-2016-07:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
113.240.250.154	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
106.1.112.199	147.237.0.19	Taiwan	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.74.129.245	147.237.77.74	Iran, Islamic Republic of	law.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
78.129.171.173	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN Potential SSH Scan	1
216.81.230.167	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.106	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
198.52.97.89	147.237.77.176	United States	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
195.143.227.35	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
192.223.76.213	147.237.77.19	Bolivia	law-forum.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
139.162.187.89	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
104.167.6.84	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
87.97.29.37	147.237.8.50	Hungary	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
220.231.195.122	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
78.129.171.173	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
210.212.207.80	147.237.0.35	India	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
195.143.227.35	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
195.143.227.35	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN NMAP -f -sS	1
185.93.185.10	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

09-26-2016-06:04:09 to 09-26-2016-07:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.152.117	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
93.169.192.220	Saudi Arabia	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
37.26.146.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.182.133	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.70.227	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.2.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.34.171	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
37.26.146.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
62.219.34.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
88.202.218.238	United Kingdom	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
65.49.2.190	United States	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	2
5.29.29.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.237	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.142	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.86.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
195.43.67.85	Poland	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.85.142	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.55.188.208	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
151.80.44.115	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
2.55.188.208	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.72	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
186.75.83.70	Panama	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.71	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.206.90	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.243	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
138.246.253.19	Germany	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
74.82.47.45	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.251.69.10	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
43.245.186.233	Indonesia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
184.105.139.75	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
71.6.167.142	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.206.116	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.247	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
138.246.253.19	Germany	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.102.218.2	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
46.19.86.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.227	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
93.169.192.220	Saudi Arabia	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
218.22.211.69	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
184.105.247.247	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
24.237.158.9	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-26-2016-06:04:09 to 09-26-2016-07:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
185.120.126.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.22	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	3
77.138.26.20	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
40.77.167.6	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
157.55.39.135	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/horaot	Block	1
80.87.205.246	Russian Federation	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name …[[#3]]•Ÿw[[#4]]3ÔÞ[[#0]][[#0]]fÀ[[#20]]À	Block	1
66.249.73.186	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/edim/yoman/enlarge.asp	Block	1
2.53.152.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
80.87.205.246	Russian Federation	147.237.77.216	dover.idf.il	NULL Character in Method [[#22]][[#3]][[#2]][[#0]]Ü[[#1]][[#0]][[#0]]Ø[[#3]][[#2]]SC[••›r[[#11]]¼[[#12]]¼+'¨H–Ï½9[[#4]]Ì[[#22]]	Block	1
77.138.87.96	France	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
40.77.167.53	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
180.76.15.148	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-ui.js	Block	1
80.87.205.246	Russian Federation	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#2]][[#0]]Ü[[#1]][[#0]][[#0]]Ø[[#3]][[#2]]SC[••›r[[#11]]¼[[#12]]¼+'¨H–Ï½9[[#4]]Ì[[#22]]	Block	1
66.249.76.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1673	Block	1
31.13.102.123	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/ https:/twitter.com/	Block	1
80.87.205.246	Russian Federation	147.237.77.216	dover.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#2]][[#0]]Ü[[#1]][[#0]][[#0]]Ø[[#3]][[#2]]SC[••›r[[#11]]¼[[#12]]¼+'¨H–Ï½9[[#4]]Ì[[#22]] in URL	Block	1
77.138.232.212	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
80.87.205.246	Russian Federation	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 4	Block	1
66.249.76.66	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/894-he	Block	1
31.154.81.2	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
85.65.244.190	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https:/twitter.com/	Block	1
80.87.205.246	Russian Federation	147.237.77.216	dover.idf.il	Abnormally Long Header Line request header name	Block	1
46.19.86.22	Israel	147.237.0.19	madim.atal.idf.il	Multiple Unauthorized URL Access from 46.19.86.22	Block	1
209.6.151.199	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/sip_storage/files/4/	Block	1
80.87.205.246	Russian Federation	147.237.77.216	dover.idf.il	Malformed URL	Block	1
66.249.76.87	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1300-he/refuah.aspx	Block	1
31.154.81.2	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
136.243.35.38	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
80.87.205.246	Russian Federation	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
2.53.147.96	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
80.87.205.246	Russian Federation	147.237.77.216	dover.idf.il	NULL Character in Header Name at À[[#19]]À#011À[[#31]]À[[#30]][[#0]]3[[#0]]2[[#0]]š[[#0]]™[[#0]]E[[#0]]DÀ[[#14]]À[[#4]][[#0]]/[[#0]]–[[#0]]AÀ[[#17]]À[[#7]]À[[#12]]À[[#2]][[#0]][[#5]][[#0]][[#4]][[#0]][[#21]][[#0]][[#18]][[#0]]#011[[#0]][[#20]][[#0]][[#17]][[#0]][[#8]][[#0]][[#6]][[#0]][[#3]][[#0]]ÿ[[#1]][[#0]][[#0]]I[[#0]][[#11]][[#0]][[4]][[#3]][[#0]][[#1]][[#2]][[#0]]	Block	1

09-26-2016-06:04:09 to 09-26-2016-07:04:09