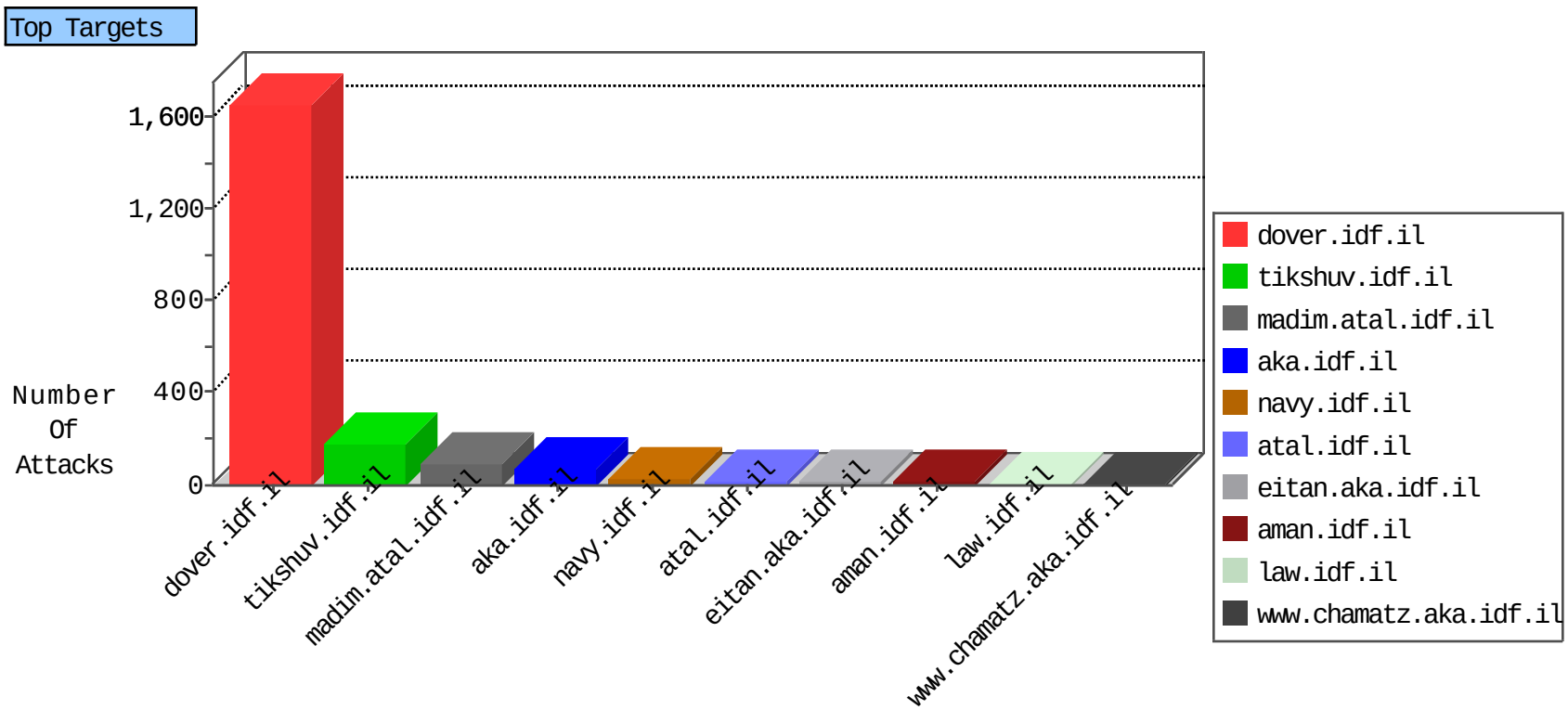
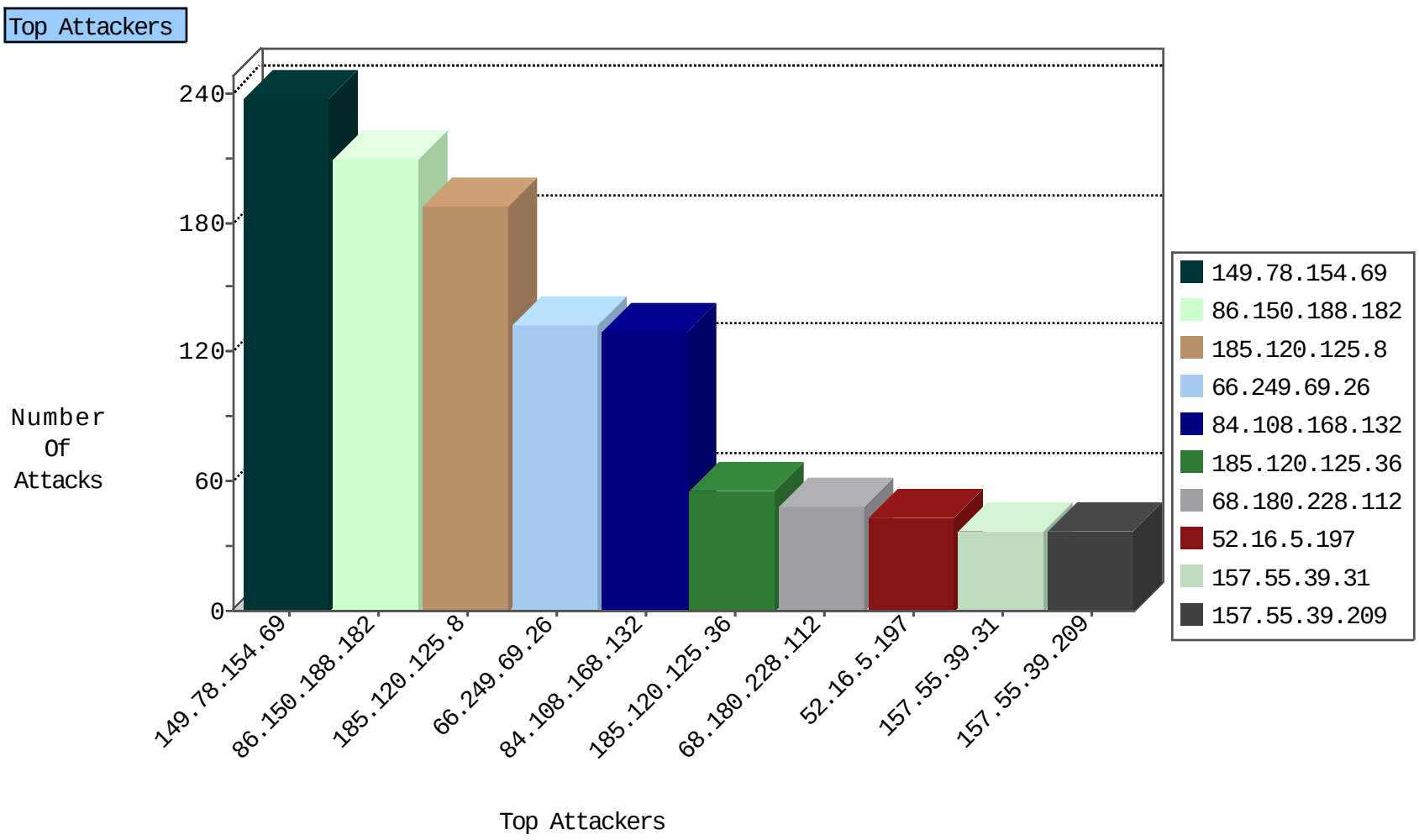
02-13-2016-09:04:05 to 02-13-2016-10:04:05

IDF Under Attack Daily Report





02-13-2016-09:04:05 to 02-13-2016-10:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
115.239.228.10	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Http	drop	2
93.174.93.218	Netherlands	147.237.77.233	atal.idf.il	block-sp-traf1	drop	2
204.42.253.132	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

02-13-2016-09:04:05 to 02-13-2016-10:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

02-13-2016-09:04:05 to 02-13-2016-10:04:05

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	3
185.110.132.54	147.237.77.179		e.mazi.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
185.110.132.54	147.237.76.147		chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
31.184.195.114	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
185.110.132.54	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
31.184.195.114	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
111.207.243.73	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.231	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 1024	1
58.177.52.70	147.237.76.31	Hong Kong	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.110.132.54	147.237.76.176		test.ncore.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
185.110.132.54	147.237.76.34		yohalan.idf.il	ET SCAN Potential SSH Scan	1
31.184.195.114	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
175.6.228.149	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
14.198.167.184	147.237.76.30	Hong Kong	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
111.207.243.73	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

02-13-2016-09:04:05 to 02-13-2016-10:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
2.52.160.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
100.127.76.238		147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.128	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
199.30.24.146	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.108.216.31	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.86.192	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
178.255.215.87	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
46.19.85.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.8.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.132.250.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.200.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.174	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.142.64.133	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
37.26.148.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.111.108.230	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.174	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.111.108.230	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.18.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.167.206	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.121	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
202.63.104.65	India	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.144	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
151.80.164.147	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
93.174.93.218	Netherlands	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
202.63.104.65	India	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
66.249.78.170	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.219	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.205	United States	147.237.0.33	idf.il	drop		drop	1
37.142.64.133	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
86.150.188.182	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
212.83.40.238	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.46	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.62.53.168	Russian Federation	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.43.111.66	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
216.218.206.88	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.179.176.96	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
202.63.104.65	India	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
68.180.229.230	United States	147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.211	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.88.118.122	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
37.142.64.133	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
86.150.188.182	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.59	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.120.130.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	236
86.150.188.182	United Kingdom	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	201
185.120.125.8		147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 185.120.125.8	Block	176
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	132
84.108.168.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	86
185.120.125.36		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	56
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	48
84.108.168.132	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	44
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	43
157.55.39.209	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	37
157.55.39.31	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	36
185.120.126.77		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	36
213.8.204.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
46.121.121.92	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	25
2.54.40.4	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
213.8.204.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
46.19.86.39	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
37.26.149.174	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
109.66.65.250	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	16
94.159.157.78	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	16
94.242.228.108	Luxembourg	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
79.183.63.9	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
185.120.125.8		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
217.66.227.124	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
46.120.249.199	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
79.177.195.75	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
79.182.136.127	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
45.35.64.142		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
79.177.0.216	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
79.176.116.249	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
86.150.188.182	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	7
87.68.150.217	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.117.40.113	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
60.234.107.179	New Zealand	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
79.179.176.96	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
2.54.164.208	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
93.157.80.254	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.253.210.134	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
77.126.203.48	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	6
84.228.184.200	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
37.19.116.116	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
77.232.50.128	Russian Federation	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 77.232.50.128	Block	5
79.178.179.72	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5

02-13-2016-09:04:05 to 02-13-2016-10:04:05