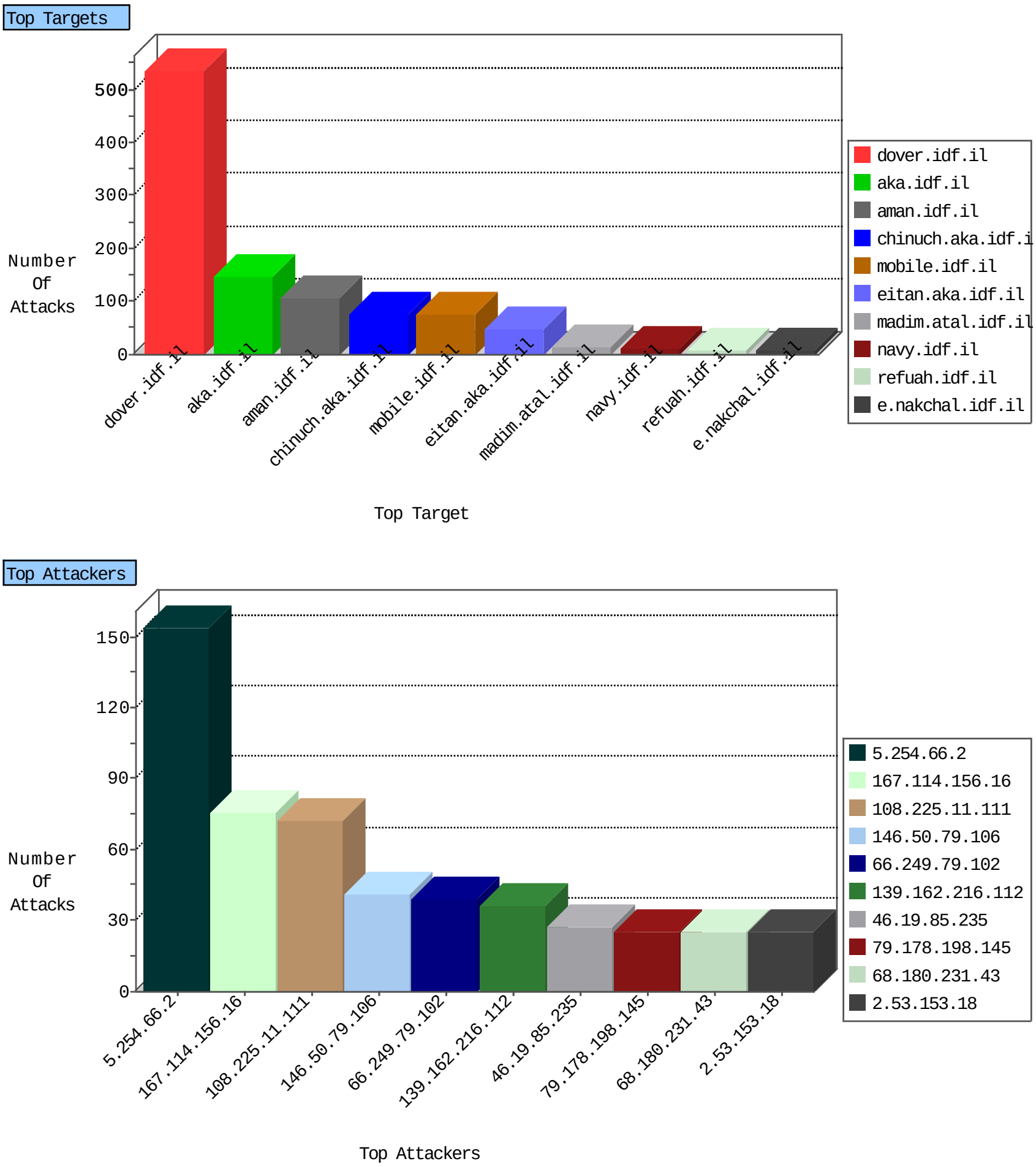
04-29-2016-19:04:06 to 04-29-2016-20:04:06

IDF Under Attack
Daily Report



04-29-2016-19:04:06 to 04-29-2016-20:04:06

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	3662
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1745
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
42.2.170.55	Hong Kong	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	2
65.38.79.88	Canada	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	2
89.46.102.242	Romania	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
71.6.146.185	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
89.46.102.242	Romania	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
58.63.6.55	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
89.46.102.242	Romania	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
82.221.105.6	Iceland	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
89.46.102.242	Romania	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
104.153.173.100	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
89.46.102.242	Romania	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1

04-29-2016-19:04:06 to 04-29-2016-20:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-29-2016-19:04:06 to 04-29-2016-20:04:06

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
80.82.78.38	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
106.184.2.29	147.237.76.39	Japan	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
212.129.15.245	147.237.77.74	France	law.idf.il	ET SCAN NMAP -sS window 1024	1
107.170.63.129	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1

04-29-2016-19:04:06 to 04-29-2016-20:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.254.66.2	Romania	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	77
5.254.66.2	Romania	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	77
108.225.11.111	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
146.50.79.106	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
66.249.79.102	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
79.178.198.145	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	25
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
109.64.87.137	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.53.153.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.235	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
208.54.38.210	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.243.150.196	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.176.127.233	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
157.55.39.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.46.41.57	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.19.222.168	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.46.41.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
87.139.165.96	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.142.68.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.71.2.88	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.247	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.127.233	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
88.254.110.197	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.3.146.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.46.39.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
100.100.57.30		147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.117.105.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
31.168.23.251	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
37.26.146.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.177.115.241	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
87.69.255.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.176.127.233	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
141.8.142.84	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.160.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-29-2016-19:04:06 to 04-29-2016-20:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.235	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
2.53.153.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.128.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.150.178.81	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.150.178.81	Block	3
109.186.52.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.46.41.57	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.142.64.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.119.113.162	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
37.142.68.1	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.2.145	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
82.80.28.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.119.113.162	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
212.150.178.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1
5.29.72.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.172	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/searchpage.aspx	Block	1
176.13.10.0	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.145.186.236	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.145.186.236	Block	1
65.55.210.61	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
213.57.139.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.168.23.251	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
141.212.122.161	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
46.119.113.162	Ukraine	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17225-he/dover.asp	Block	1
84.145.186.236	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.142	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
213.57.251.102	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
146.50.79.106	Netherlands	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1392-en/cogat.asp	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
46.119.113.162	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.119.113.162	Block	1
208.90.57.196	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
2.53.22.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
84.228.211.212	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/general/mobile	Block	1
66.249.64.154	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
148.251.70.201	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
79.180.134.29	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
66.249.64.163	Israel	147.237.76.86	navy.idf.il	Parameter Type Violation DocID in www.navy.idf.il/navy/general.aspx	Block	1

04-29-2016-19:04:06 to 04-29-2016-20:04:06