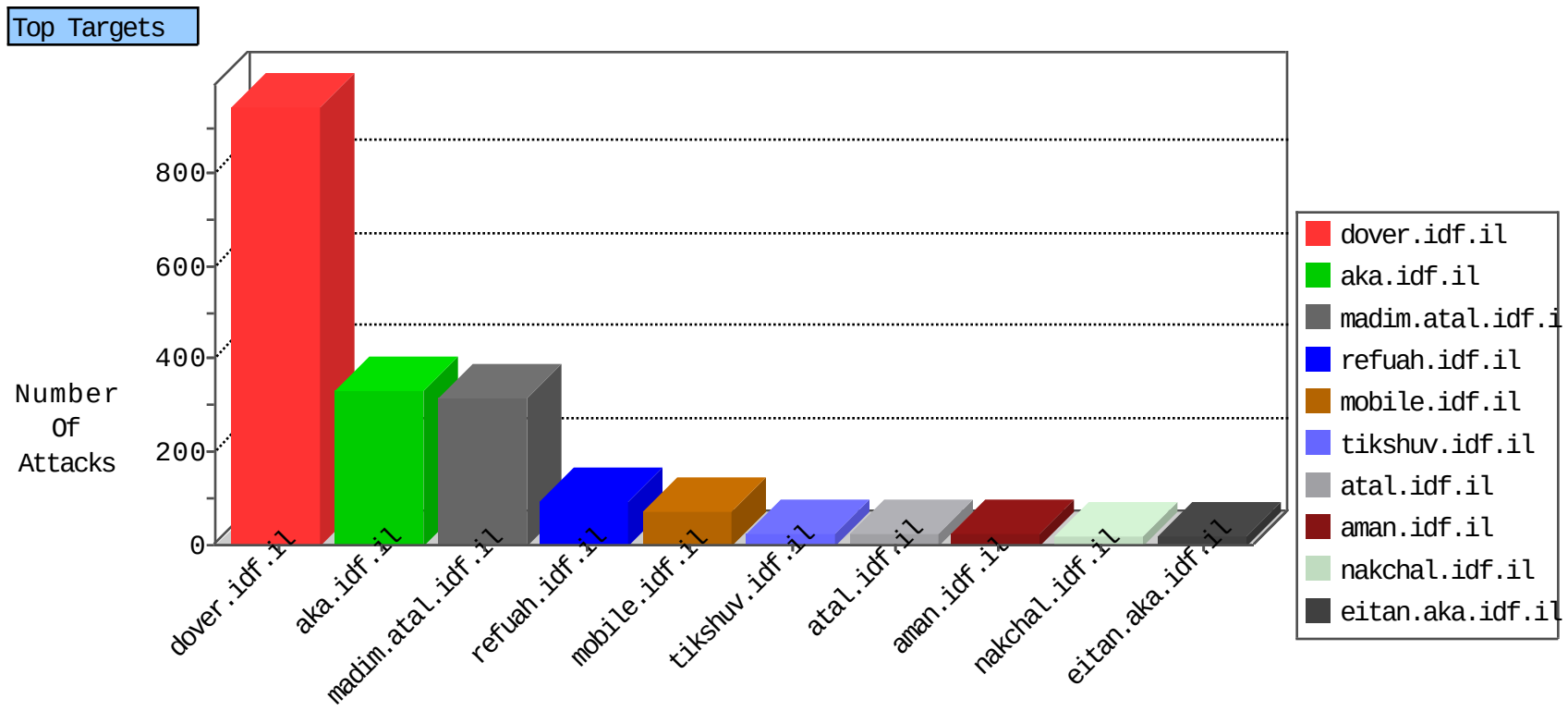
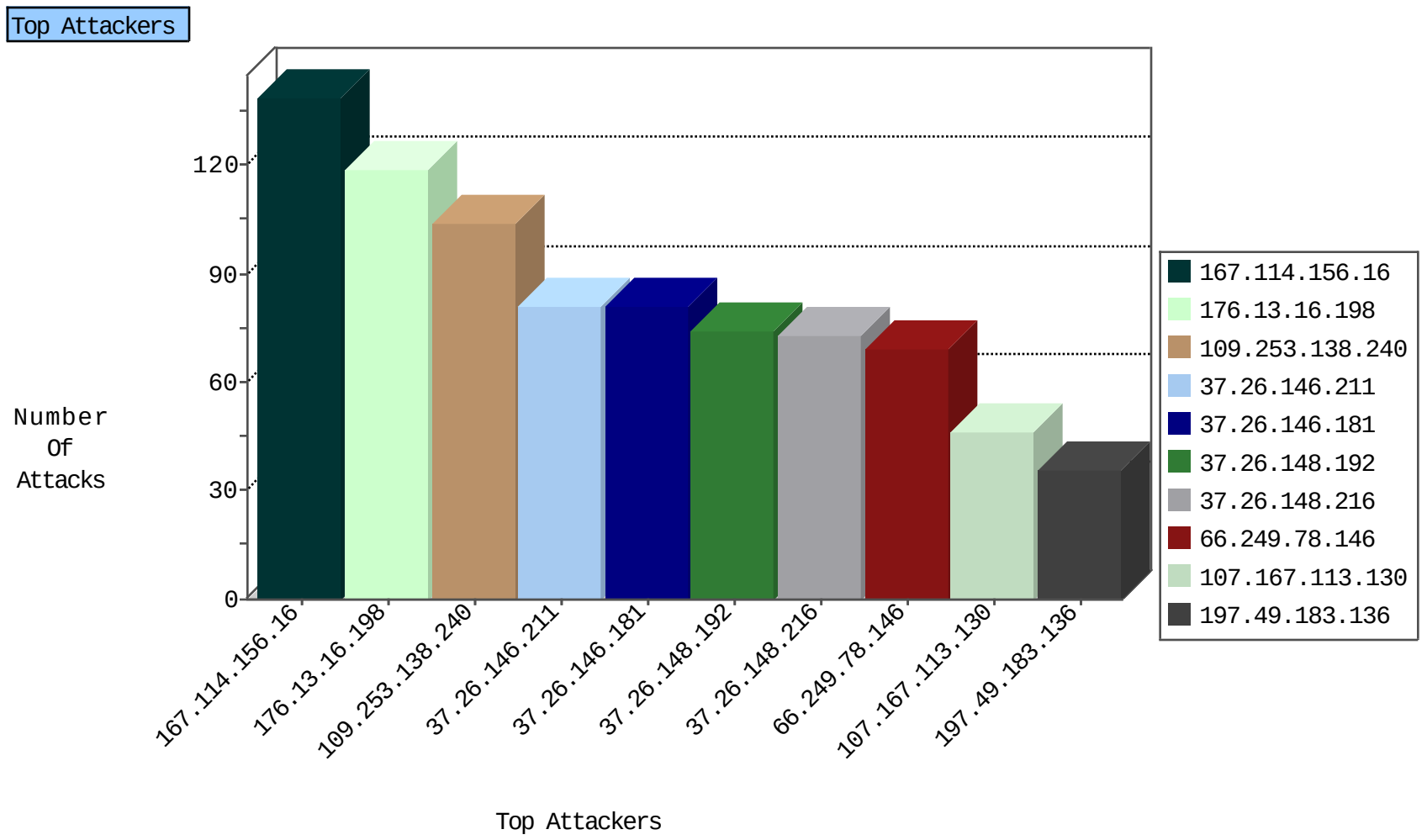
05-01-2016-19:04:05 to 05-01-2016-20:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-01-2016-19:04:05 to 05-01-2016-20:04:05

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	5024
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2418
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4
37.60.44.251	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
89.46.102.242	Romania	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
123.59.59.52	China	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
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	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.147	chinuch.aka.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
66.249.66.12	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1
89.46.102.242	Romania	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
123.59.59.52	China	147.237.0.19	madim.atal.idf.il	block-sp-traf1	drop	1
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1

05-01-2016-19:04:05 to 05-01-2016-20:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-01-2016-19:04:05 to 05-01-2016-20:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.i	Tehila - Perl LWP with fake user agent	4
46.120.65.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.132.62.181	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
109.186.35.199	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
95.86.83.217	147.237.72.166	Israel	aka.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
46.121.89.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.198	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
217.132.90.233	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
212.199.104.190	147.237.77.216	Israel	dover.idf.i	portscan: TCP Distributed Portscan	1
128.199.63.64	147.237.77.74	Netherlands	law.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
109.65.60.140	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.230.17.230	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

05-01-2016-19:04:05 to 05-01-2016-20:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.146.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
37.26.148.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
37.26.148.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	68
37.26.146.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
107.167.113.130	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	46
197.49.183.136	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
46.19.85.229	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
46.19.85.83	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	26
31.210.187.192	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
82.145.208.198	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.53.1.61	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
72.89.38.126	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
176.13.16.198	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.67.141.82	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.55.38.219	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
66.249.79.82	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.53.23.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.55.25.89	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.17.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.203.136.241	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.203.185.139	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.146.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.188.54.17	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.146.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
109.253.195.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.188.54.17	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	8
197.45.132.217	Egypt	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
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.246.130.39	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.116.130.229	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	7
46.116.130.229	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
209.133.111.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.168.84.16	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.79.84	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.217	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

05-01-2016-19:04:05 to 05-01-2016-20:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.138.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	102
176.13.16.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	97
85.65.55.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	32
79.177.217.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
2.53.43.70	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
2.53.4.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
81.218.55.253	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/9/1709.pdf	Block	4
2.53.1.61	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.66.50.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.181.56.48	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	3
176.13.15.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
157.55.39.106	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.146.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.22.135.171	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.22.135.171	Block	2
109.253.138.240	Israel	147.237.0.19	madim.atal.idf.i	Cookie Tampering on cookie Login: Expected ********** *, Observed **********	None	2
176.13.3.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.102.195.137	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$passwordUpdate$hiddenUpdatePassword in www.aka.idf.il/main/giyus/faq.aspx	None	1
94.199.151.22	United Kingdom	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 94.199.151.22	Block	1
195.154.199.235	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyusmaster/script	Block	1
109.253.196.81	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
79.181.56.48	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	1
66.249.79.52	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/8/1548.jpg	Block	1
94.199.151.22	United Kingdom	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/templates/general/general.aspx	Block	1
31.210.187.192	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
79.177.217.14	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kamlar	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method em55 in URL	Block	1
2.53.132.163	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.230.184	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1133-he/atal.aspx	Block	1
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
79.179.130.199	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
213.8.204.80	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
176.9.127.69	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
85.64.64.81	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
77.125.114.168	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
46.116.130.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
195.60.232.57	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/113484.pdf	Block	1
37.26.146.217	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.79.48	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/robots.txt	Block	1
46.19.85.158	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
5.22.135.171	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
79.177.158.120	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
65.55.213.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

05-01-2016-19:04:05 to 05-01-2016-20:04:05