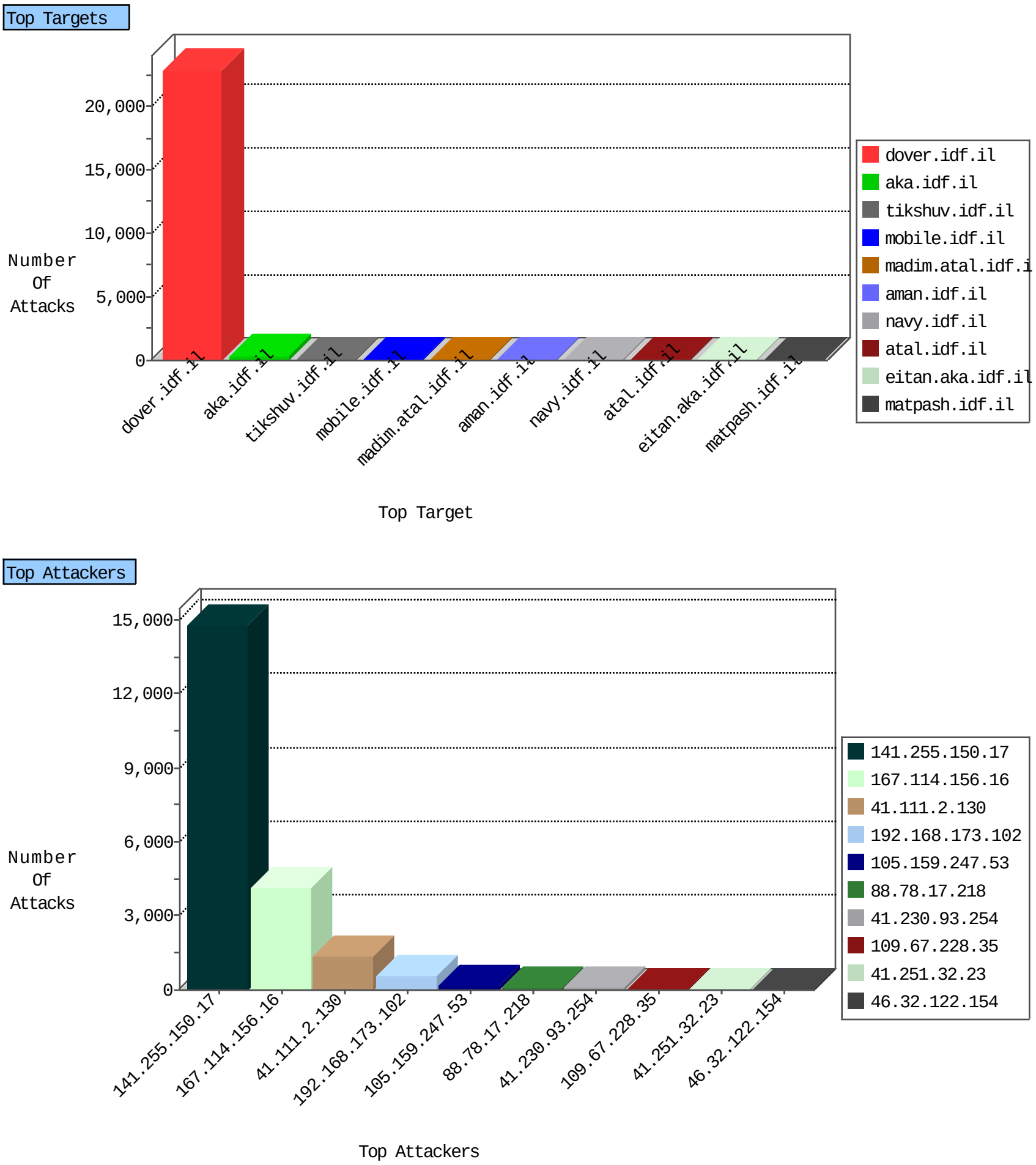
04-09-2016-23:04:01 to 04-10-2016-00:04:01

IDF Under Attack Daily Report



04-09-2016-23:04:01 to 04-10-2016-00:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	44641
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4100
141.255.150.17	Netherlands	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1549
41.111.2.130	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1354
141.255.150.17	Netherlands	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	234
141.255.150.17	Netherlands	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	102
66.249.93.111	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	84
141.255.150.17	Netherlands	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	66
105.154.186.206	Morocco	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	23
105.148.253.96	Morocco	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Product	dest-reset	20
141.255.150.17	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
62.90.49.25	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
82.145.216.237	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
95.85.51.71	Netherlands	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
69.30.198.146	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
74.91.23.108	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	2
173.208.197.252	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	2
74.91.17.178	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
105.148.253.96	Morocco	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	2
173.208.197.253	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	2
74.91.18.43	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	2
74.91.23.106	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
41.251.32.23	Morocco	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
173.208.197.252	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	forward	2
185.56.28.67	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
82.145.219.117	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1
185.56.28.67	Netherlands	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
197.0.64.52	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
176.31.60.249	France	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
95.85.51.71	Netherlands	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
82.145.217.136	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	1

04-09-2016-23:04:01 to 04-10-2016-00:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.230.9	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
37.26.147.227	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
149.78.68.52	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
151.80.31.180	France	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
141.255.150.17	Netherlands	147.237.77.216	dover.idf.il	10725: TCP: LOIC DDoS Tool	Block	1

04-09-2016-23:04:01 to 04-10-2016-00:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.205.111.236	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	4
66.249.65.224	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
185.114.157.12	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
185.114.157.12	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -f -sS	1
141.255.150.17	147.237.77.216	Netherlands	dover.idf.il	ET CURRENT_EVENTS Inbound Low Orbit Ion Cannon LOIC DDOS Tool desu string	1
91.201.236.114	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
45.79.137.87	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.76.86	United States	navy.idf.il	ET DROP Dshield Block Listed Source	1
193.201.227.117	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.114.157.12	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
176.13.15.99	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
139.162.192.213	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1

04-09-2016-23:04:01 to 04-10-2016-00:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.255.150.17	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12845
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	362
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	173
105.159.247.53	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	152
88.78.17.218	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	121
41.230.93.254	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
109.67.228.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
46.32.122.154	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
95.85.51.71	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
91.246.113.146	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
105.148.253.96	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
77.124.3.254	Israel	147.237.0.34	tikshuv.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
37.238.112.79	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
105.155.33.234	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
41.254.9.253	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
41.251.32.23	Morocco	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	22
109.186.49.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
197.19.94.71	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
2.55.57.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
37.26.146.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
109.65.68.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
79.179.198.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.117.135.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.67.4.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.108.111.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
2.52.187.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.251.32.23	Morocco	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	13
109.65.100.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
95.86.65.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.66.7.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.238.136.200	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
75.68.81.150	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
109.253.205.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
197.150.99.130	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
212.179.246.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
198.144.107.90	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.46.13.47	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.179.208.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.50.81.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
80.178.1.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
2.52.146.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.179.5.219	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

04-09-2016-23:04:01 to 04-10-2016-00:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
77.127.2.50	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	9
77.127.2.50	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.127.2.50	Block	7
85.65.96.172	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 85.65.96.172	Block	5
79.178.165.157	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Parameter Encoding from 79.178.165.157	None	5
109.67.8.24	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.67.8.24	Block	4
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
79.183.107.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	3
185.89.217.227	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
156.208.20.43	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	2
105.159.247.53	Morocco	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
77.127.2.50	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/4/	Block	2
80.246.130.145	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/71538.pdf	Block	1
41.40.140.194	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.64.27.202	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
79.178.165.157	Israel	147.237.72.156	aman.idf.il	NULL Character in Parameter Value at 1 for www.aman.idf.il/modiin/kiosk.aspx	Block	1
197.0.64.52	Tunisia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar cmdping -t6500 147.237.77.21lestine	Block	1
173.208.197.252	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to www.tt985.com/	Block	1
105.104.130.12	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
41.251.32.23	Morocco	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /sip_storcn e/cileq/3/qize2±0x52[[#15]]17µ23(j•g"¸tts/q.2•	Block	1
80.246.130.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.29.123.133	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.29.123.133	Block	1
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20420-he/dover.aspx	Block	1
41.45.127.34	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
85.65.11.117	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/https:/mobile.idf.il/	Block	1
79.179.198.245	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
197.15.72.24	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/il/	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8871-he/refuah.aspx	Block	1
173.208.197.252	United States	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on www.tt985.com/	Block	1
41.251.32.23	Morocco	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
80.246.130.210	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.29.123.133	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/sachar/default.aspx	Block	1
66.249.78.127	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/forums.frm/frmuserdetails.aspx	Block	1
157.55.39.109	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
41.142.28.83	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
69.30.198.146	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to www.tt985.com/	Block	1
173.208.197.253	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.tt985.com/	Block	1
105.159.247.53	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.159.247.53	Block	1
45.33.136.30	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
84.111.248.101	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.89.217.234	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.178.163.143	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
66.249.78.134	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
157.55.39.211	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/general.aspx	Block	1
41.251.32.23	Morocco	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name Accfðt	Block	1
85.65.96.172	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	1

04-09-2016-23:04:01 to 04-10-2016-00:04:01