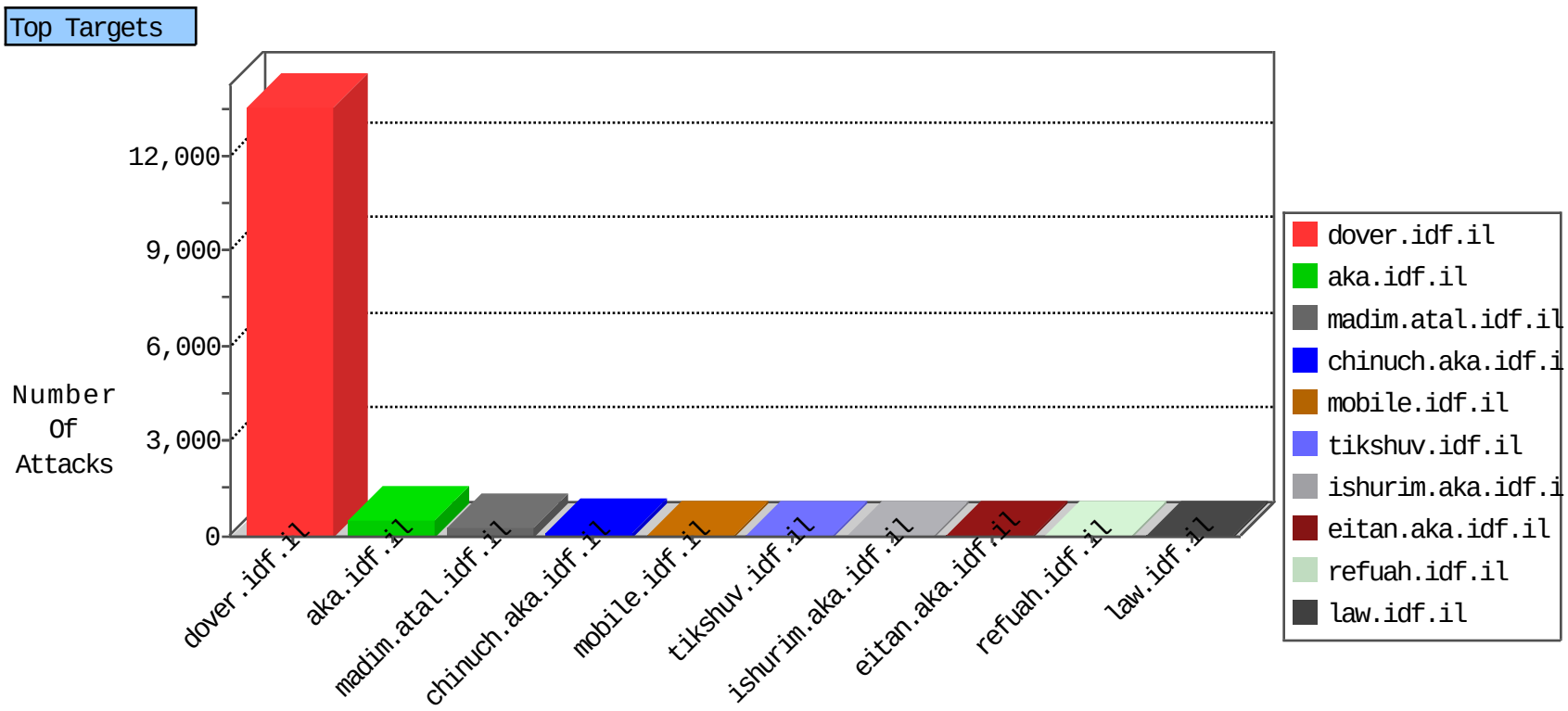
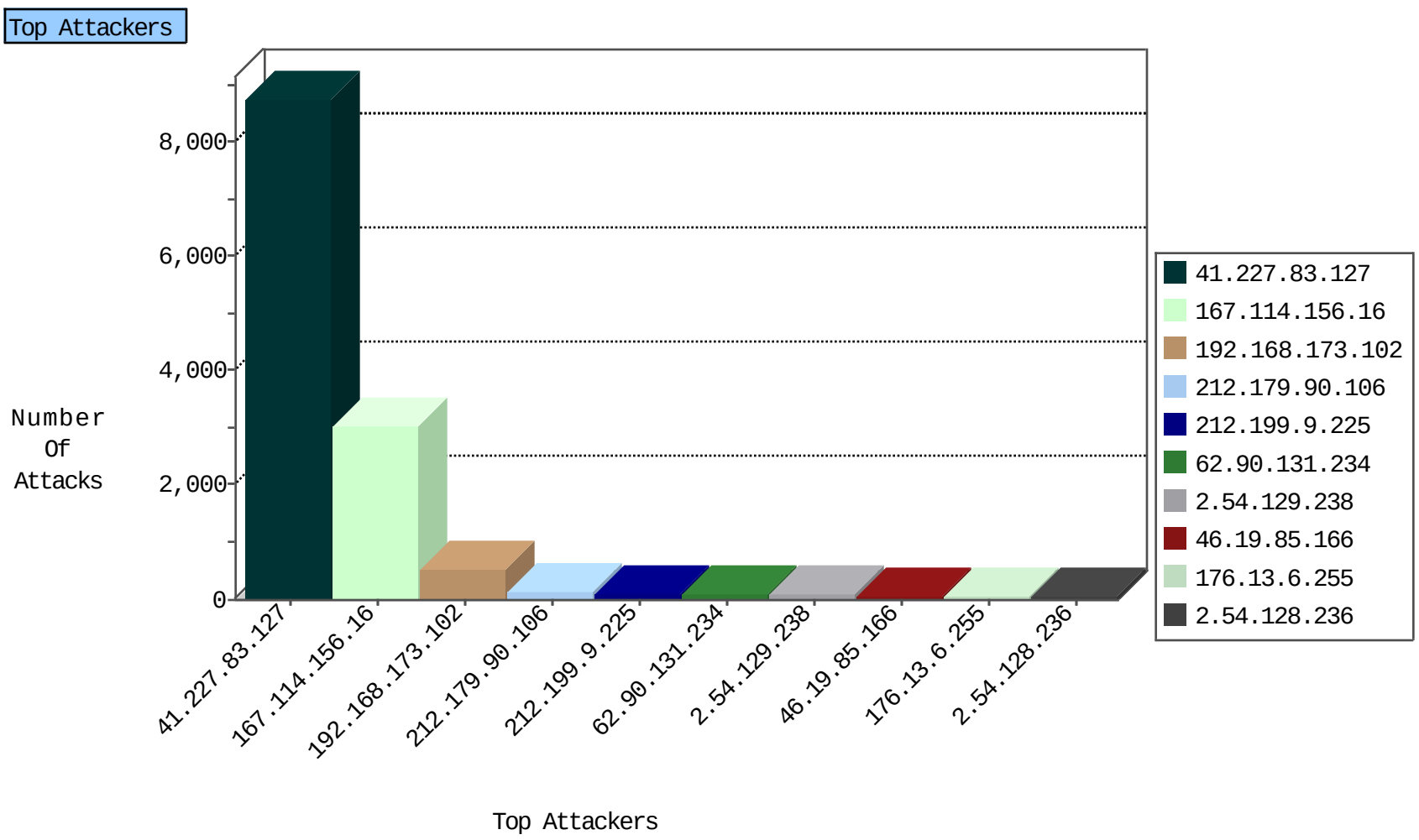
04-10-2016-15:04:04 to 04-10-2016-16:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-10-2016-15:04:04 to 04-10-2016-16:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3477
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3022
47.17.214.150	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	692
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	395
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	88
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	13
81.218.150.163	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
81.218.206.82	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
132.72.172.185	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
192.0.83.17	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
107.150.32.58	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
74.91.18.42	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	2
69.30.198.147	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
69.30.226.221	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
107.150.46.35	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
74.91.23.108	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
69.30.202.227	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	2
173.208.197.253	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
69.197.185.19	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	2
80.74.107.118	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
69.30.202.229	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
101.201.147.32	China	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	2
74.91.17.179	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
69.30.198.146	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
69.30.226.219	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	2
46.19.86.216	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.143.133.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
2.52.128.24	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
91.202.129.171	Ukraine	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
62.90.35.162	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
109.64.150.135	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
188.135.47.66	Oman	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-10-2016-15:04:04 to 04-10-2016-16:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.170.254	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
79.176.89.80	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
80.74.110.129	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
149.78.206.16	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
212.143.103.202	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
193.106.206.10	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.120.23.206	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-10-2016-15:04:04 to 04-10-2016-16:04:04

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	1
109.253.202.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.173.14.114	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.22.181	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
83.235.181.57	147.237.76.196	Greece	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
77.124.7.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.7.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.52.7	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.180.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.193.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
83.235.181.57	147.237.76.196	Greece	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
79.179.188.236	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.160	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1

04-10-2016-15:04:04 to 04-10-2016-16:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7751
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	362
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	drop		drop	313
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	183
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	137
212.199.9.225	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	105
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	91
2.54.129.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	77
176.13.6.255	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
176.13.19.113	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
212.235.2.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
207.241.229.224	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.103	Israel	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	28
185.27.105.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
46.19.85.245	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	26
46.19.85.193	Israel	147.237.76.86	navy.idf.il	drop	SAM rule	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
81.218.24.90	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
81.218.245.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
67.84.157.191	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
212.143.186.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
213.8.204.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
149.88.34.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.67.170.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.131.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.69.221.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.150.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.120.84.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.142.64.54	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
192.114.23.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
213.151.35.221	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
172.98.67.135	Canada	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.114.23.18	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.186.49.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.160	Israel	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	9
176.13.0.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.54.167.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
149.88.189.240	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.54.170.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8

04-10-2016-15:04:04 to 04-10-2016-16:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.90.131.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
46.19.85.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
2.54.128.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
109.253.142.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
176.13.18.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.86.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
62.219.99.154	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	11
132.76.50.5	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	9
62.219.99.154	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 62.219.99.154	Block	8
185.32.179.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
132.74.58.51	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 132.74.58.51	Block	4
31.168.96.254	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 31.168.96.254	Block	4
131.253.25.142	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
131.253.25.207	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.220.139	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
82.80.135.182	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
82.80.135.182	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/7/	Block	1
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
74.91.17.179	United States	147.237.76.200	eitan.aka.idf.il	Distributed Unauthorized URL Access on www.app-softwares.com/	Block	1
2.54.128.236	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ********** ********** ********** **********, Observed ********** ********** ********** **********	None	1
194.90.66.9	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
141.212.122.129	United States	147.237.77.235	sviva.idf.il	Unauthorized URL Access to /x	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
107.150.46.35	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.ps780.com/	Block	1
37.8.118.193	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
212.199.112.144	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1407-he/atal.aspx	Block	1
81.218.24.90	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
69.30.198.146	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.app-softwares.com/	Block	1
185.27.105.165	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/favicon.ico	Block	1
62.219.99.154	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	1
82.81.78.139	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb13697877 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvs=570a436573a5708d000	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/13108.jpg	Block	1
74.91.18.42	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.ps780.com/	Block	1
173.208.197.253	United States	147.237.76.39	mobile.meitav.idf.i	Distributed Unauthorized URL Access on www.app-softwares.com/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;innerCatID in www.aka.idf.il/giyus/qanda/default.asp	None	1
46.19.86.143	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/default.aspx	Block	1
41.100.133.129	Algeria	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
213.151.62.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
82.80.27.25	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation searchText in www.atal.idf.il/1559-he/atal.aspx	Block	1
69.30.202.229	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.369bs.com/	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
85.130.221.188	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Malformed URL __atuvc=1	Block	1
2.54.196.144	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/8/size220x0/13108.jpg	Block	1
74.91.23.108	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.app-softwares.com/	Block	1
176.13.6.255	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
41.100.133.129	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin	Block	1

04-10-2016-15:04:04 to 04-10-2016-16:04:04