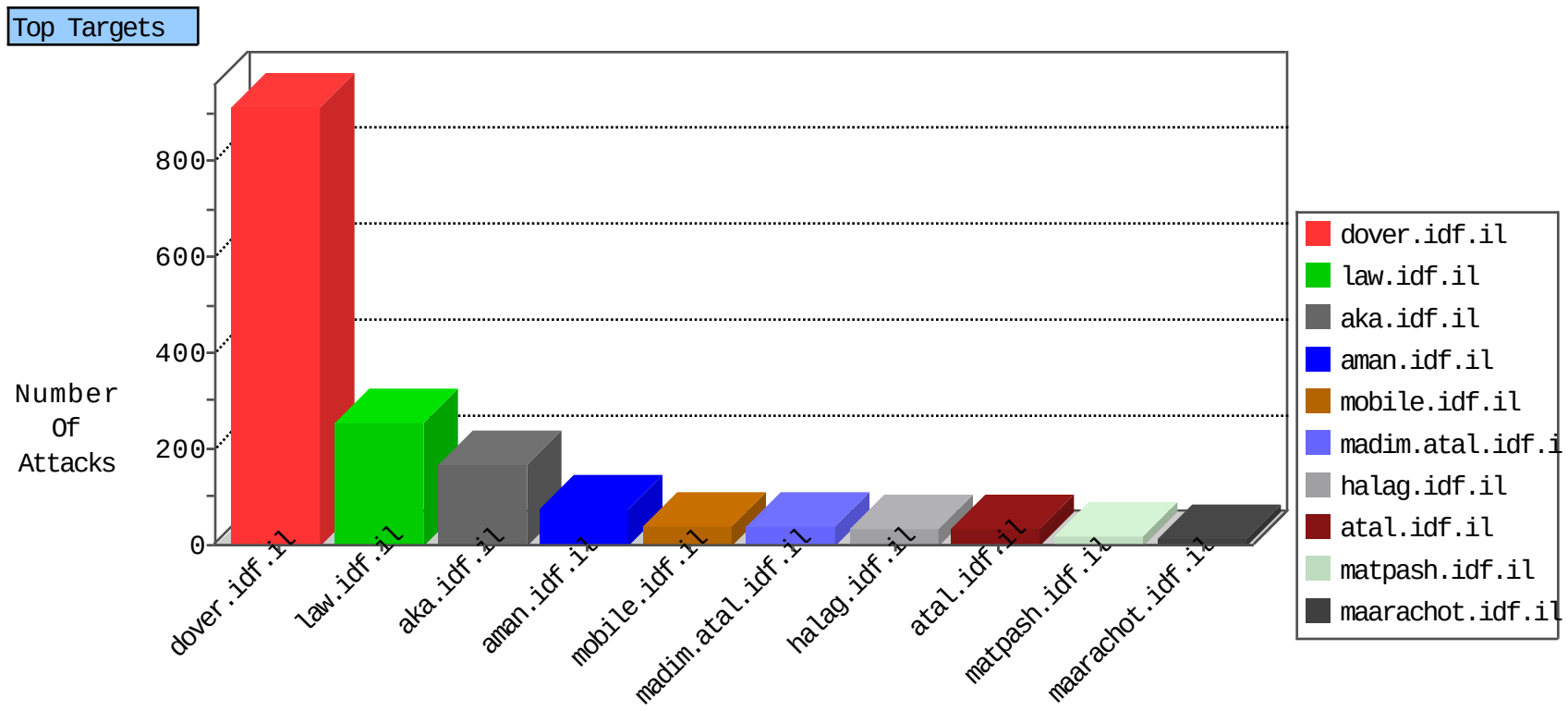
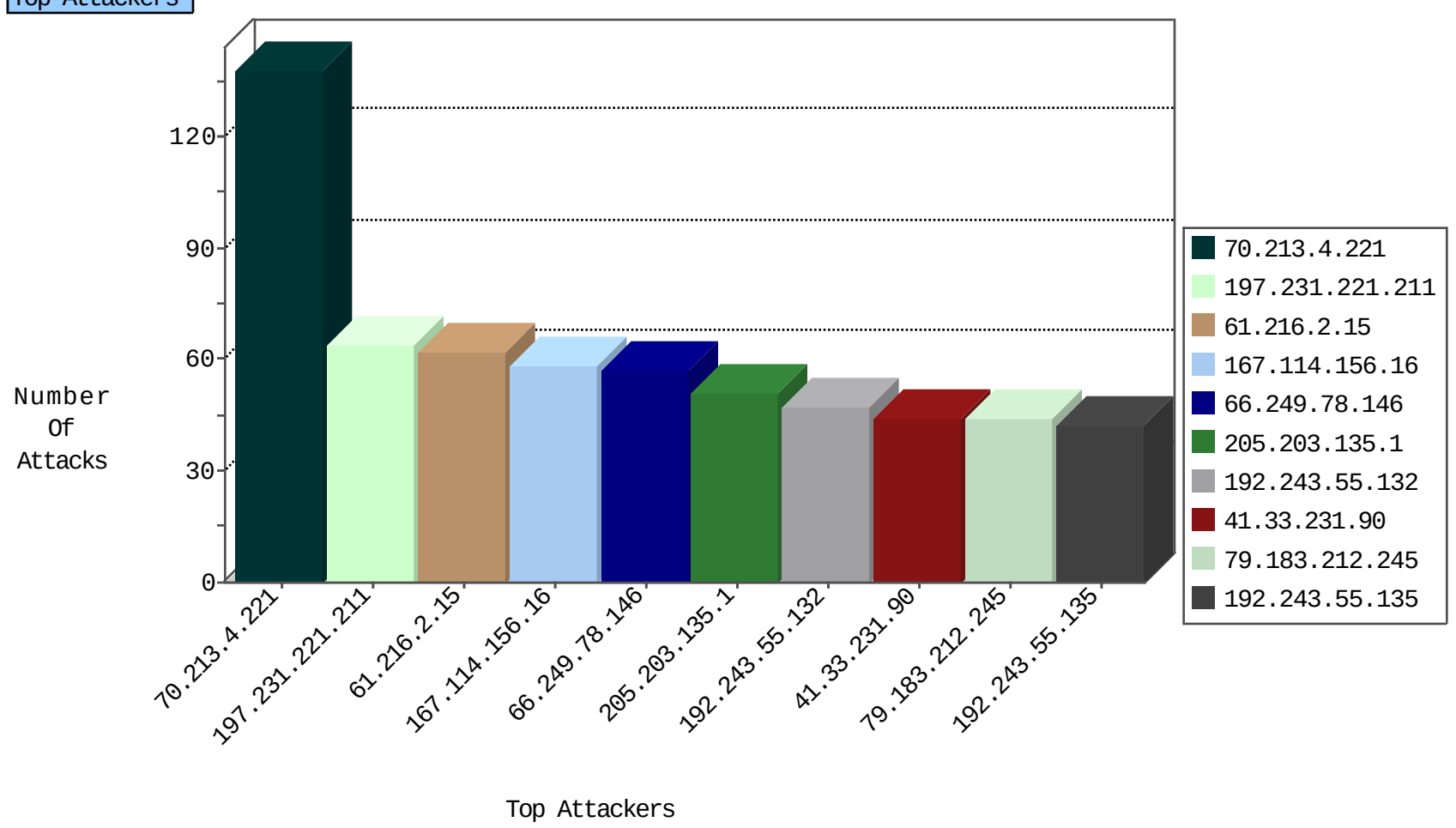
04-22-2016-16:04:04 to 04-22-2016-17:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-22-2016-16:04:04 to 04-22-2016-17:04:04

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-POST-Segmented-DoS	dest-reset	2551
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1687
31.168.176.104	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
199.115.117.88	United States	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Https	drop	1
94.102.52.10	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1

04-22-2016-16:04:04 to 04-22-2016-17:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-22-2016-16:04:04 to 04-22-2016-17:04:04

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	4
213.192.3.1	147.237.76.202	Czech Republic	e.halag.idf.il	ET SCAN Potential SSH Scan	2
213.192.3.1	147.237.77.61	Czech Republic	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
89.248.162.175	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
213.192.3.1	147.237.76.200	Czech Republic	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
89.139.156.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.192.3.1	147.237.76.148	Czech Republic	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
79.177.120.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.192.3.1	147.237.76.31	Czech Republic	nakchal.idf.il	ET SCAN Potential SSH Scan	1
213.192.3.1	147.237.72.156	Czech Republic	aman.idf.il	ET SCAN Potential SSH Scan	1
213.192.3.1	147.237.77.235	Czech Republic	sviva.idf.il	ET SCAN Potential SSH Scan	1
146.0.79.211	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
213.192.3.1	147.237.77.227	Czech Republic	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
213.192.3.1	147.237.77.212	Czech Republic	e.dover.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
89.248.162.175	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
213.192.3.1	147.237.76.196	Czech Republic	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
84.200.15.174	147.237.77.170	Germany	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
213.192.3.1	147.237.76.34	Czech Republic	yohalan.idf.il	ET SCAN Potential SSH Scan	1
23.125.172.41	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
213.192.3.1	147.237.72.166	Czech Republic	aka.idf.il	ET SCAN Potential SSH Scan	1
195.154.54.169	147.237.0.15	France	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.252.84	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
213.192.3.1	147.237.77.234	Czech Republic	halag.idf.il	ET SCAN Potential SSH Scan	1
111.65.174.3	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
213.192.3.1	147.237.77.226	Czech Republic	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1

04-22-2016-16:04:04 to 04-22-2016-17:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
70.213.4.221	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	138
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
66.87.31.164	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
79.181.187.151	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	33
95.86.104.64	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
91.121.221.15	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
79.183.212.245	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
79.183.212.245	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
213.57.48.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
138.207.151.67	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
79.178.136.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
69.139.45.52	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
207.46.13.14	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
162.243.71.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
157.55.39.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
157.55.39.230	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
189.122.130.131	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
61.216.2.15	Taiwan	147.237.77.170	maarachot.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	9
213.57.48.147	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	9
176.13.12.129	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.179.217.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.132	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.135	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
99.233.129.107	Canada	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
105.203.254.2	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7

04-22-2016-16:04:04 to 04-22-2016-17:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.5.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
176.13.12.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
72.18.194.32	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 72.18.194.32	Block	5
79.178.136.100	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
105.203.254.9	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
105.203.254.10	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
31.168.176.104	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	2
157.55.39.230	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
61.216.2.15	Taiwan	147.237.77.234	halag.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
31.13.112.118	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-8329-he/dover.aspx&ved=0ahukewixzjyarqlmahvj1ywkhapwbqaqfggzmaa&usg=afqjcnenol0cyyqa2o8npxv8mguifl-s0q	Block	1
80.230.218.85	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
186.45.28.38	Trinidad and Tobago	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
61.216.2.15	Taiwan	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 61.216.2.15	Block	1
109.253.150.136	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
105.203.254.7	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
61.216.2.15	Taiwan	147.237.77.235	sviva.idf.il	Illegal Byte Code Character in Method	Block	1
105.203.254.11	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.65.109.18	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
186.45.28.38	Trinidad and Tobago	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
61.216.2.15	Taiwan	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
131.253.25.169	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 131.253.25.169	Block	1
105.203.254.8	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.183.212.245	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.87.31.164	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.idf.il/1038-en/dover.aspx	Block	1
46.19.85.213	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
105.203.254.13	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.248.227.163	Slovakia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
72.18.194.32	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
193.34.208.10	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/general/mobile	Block	1
131.253.25.169	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
61.216.2.15	Taiwan	147.237.77.226	www.chamatz.aka.idf.il	Illegal Byte Code Character in Method	Block	1
105.203.254.8	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
80.230.218.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
184.105.247.195	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.78.4	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
61.216.2.15	Taiwan	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in Method from 61.216.2.15	Block	1
105.203.254.15	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.69.81.189	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
74.216.182.82	Canada	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
207.46.13.162	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
141.212.122.161	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1
61.216.2.15	Taiwan	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Method	Block	1
5.29.179.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
80.230.218.84	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	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
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
61.216.2.15	Taiwan	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in Method	Block	1
107.150.32.62	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
105.203.254.4	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

04-22-2016-16:04:04 to 04-22-2016-17:04:04