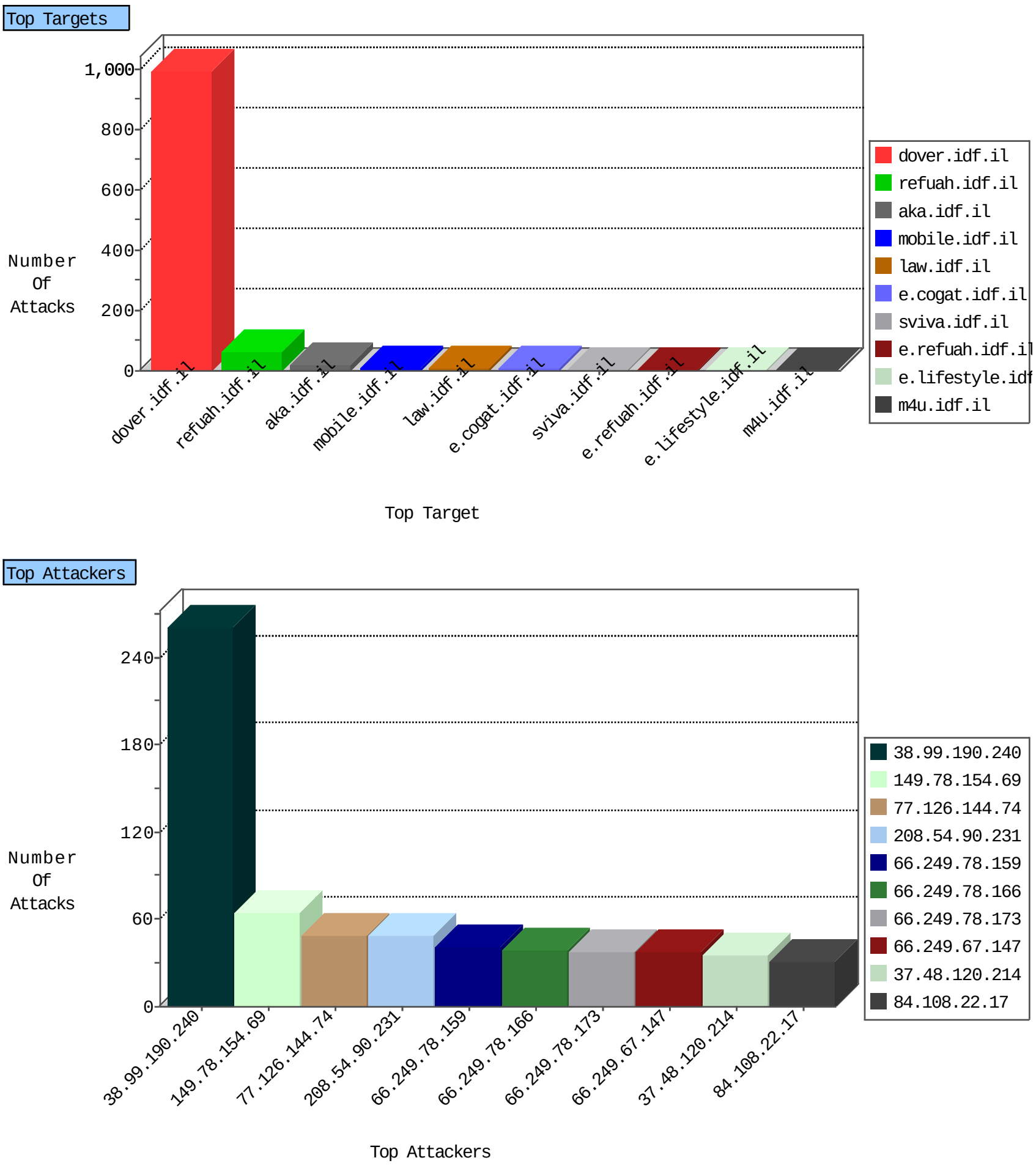
05-06-2015-02:03:09 to 05-06-2015-03:03:09

IDF Under Attack
05-06-2015-02:03:09



05-06-2015-02:03:09 to 05-06-2015-03:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.64.153	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	684
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
222.186.56.178	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
104.255.66.201		147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
61.194.80.107	Japan	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

05-06-2015-02:03:09 to 05-06-2015-03:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	23
188.138.9.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1

05-06-2015-02:03:09 to 05-06-2015-03:03:09

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.67.147	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	38
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
113.21.226.56	New Zealand	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.244	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.244	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
31.184.194.114	Russian Federation	147.237.77.235	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.235.189.244	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	Cote D'Ivoire	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 2048	1
188.138.9.51	Germany	147.237.77.74	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
188.138.9.51	Germany	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.178	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
92.47.29.12	Kazakstan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.244	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.244	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
31.184.194.114	Russian Federation	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.235.189.244	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	Cote D'Ivoire	147.237.72.166	aka.idf.il	ET SCAN NMAP -f -sS	1
188.138.9.51	Germany	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
188.138.9.51	Germany	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1

05-06-2015-02:03:09 to 05-06-2015-03:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
38.99.190.240	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	259
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
77.126.144.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
208.54.90.231	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
84.108.22.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
108.64.228.151	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
31.168.90.18	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	20
217.65.199.83		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
82.145.210.25	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
46.120.31.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
217.65.199.82		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
68.189.92.202	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
37.216.6.219	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
217.65.199.88		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
46.19.86.167	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
217.65.199.86		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
157.55.39.135	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
107.3.176.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
74.107.99.100	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
104.35.90.139		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
217.65.199.85		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
37.247.36.108	Netherlands	147.237.77.61	e.cogat.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	5
191.181.157.211	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
77.126.90.151	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
80.246.133.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
217.65.199.84		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.64.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
188.165.15.99	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
79.176.24.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.64.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
198.100.144.55	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
108.162.47.122	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
68.180.229.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.179.23.22	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
54.147.176.220	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
157.55.39.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2

05-06-2015-02:03:09 to 05-06-2015-03:03:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	8
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	6
188.120.142.233	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 188.120.142.233	Block	3
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	3
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
188.120.142.233	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
52.6.169.50	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	2
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	1
37.142.156.172	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
202.46.57.105	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.73.229	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.235	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/981-he/patzar.aspx	Block	1
46.19.123.125	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.81	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1132-8613-he/navy.aspx.aspx	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19798-he/idfgdover.aspx	Block	1
61.135.190.71	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20477-he/dover.aspx	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sachar/forms/downloadform.asp	Block	1
46.120.70.189	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
61.135.190.200	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
188.138.17.205	France	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
77.237.138.51	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized URL Access to /	Block	1
66.249.67.218	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1312-he/refuah.aspx	Block	1
207.46.13.78	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/news.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14137-he/mmmmmmm=277c243dmmmmmmm_277c243d	Block	1
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	1
188.165.15.99	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0126-2.stm	Block	1
79.181.177.91	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.73.209	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
210.187.213.90	Malaysia	147.237.77.216	dover.idf.il	Distributed eMail Hoarding	Block	1
54.147.176.220	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.61.138.244		147.237.0.15	kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

05-06-2015-02:03:09 to 05-06-2015-03:03:09