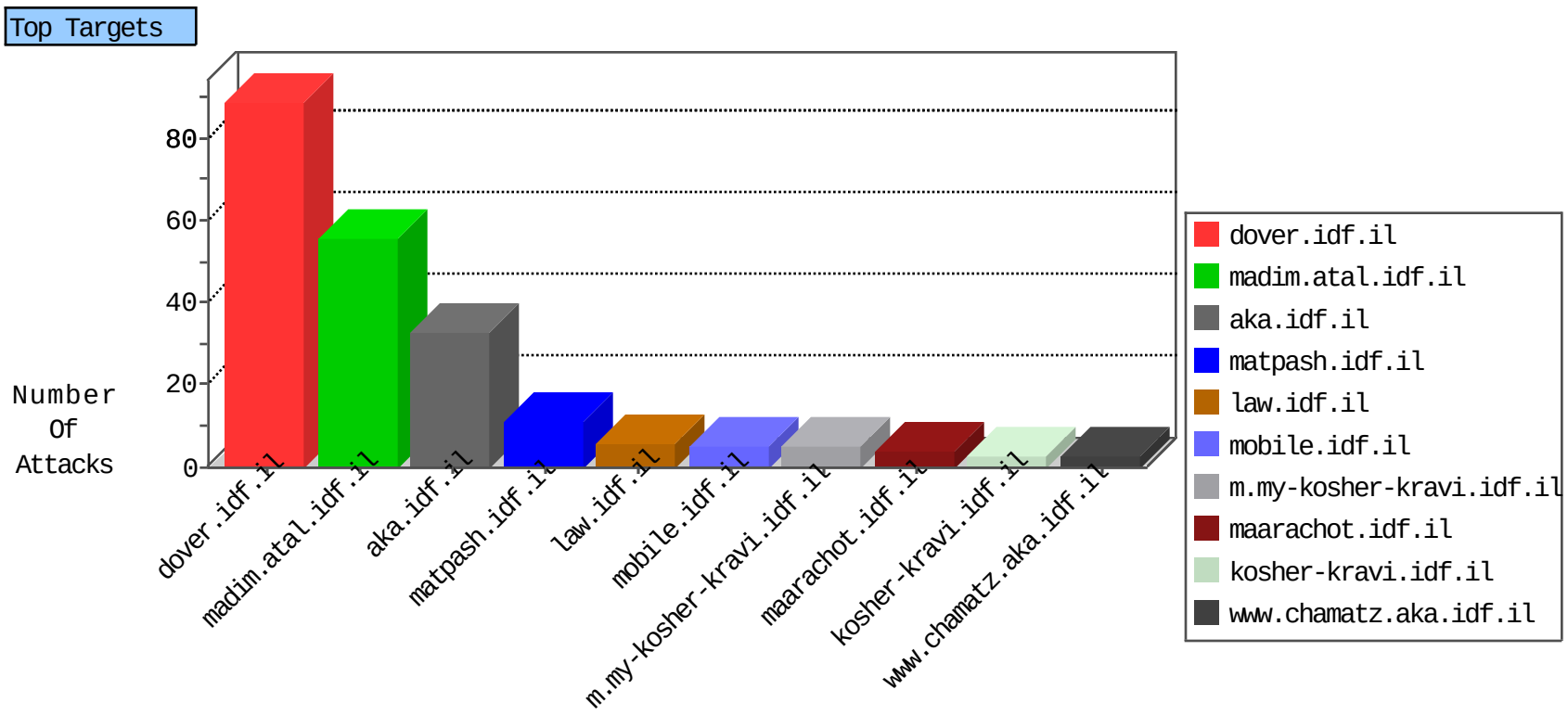
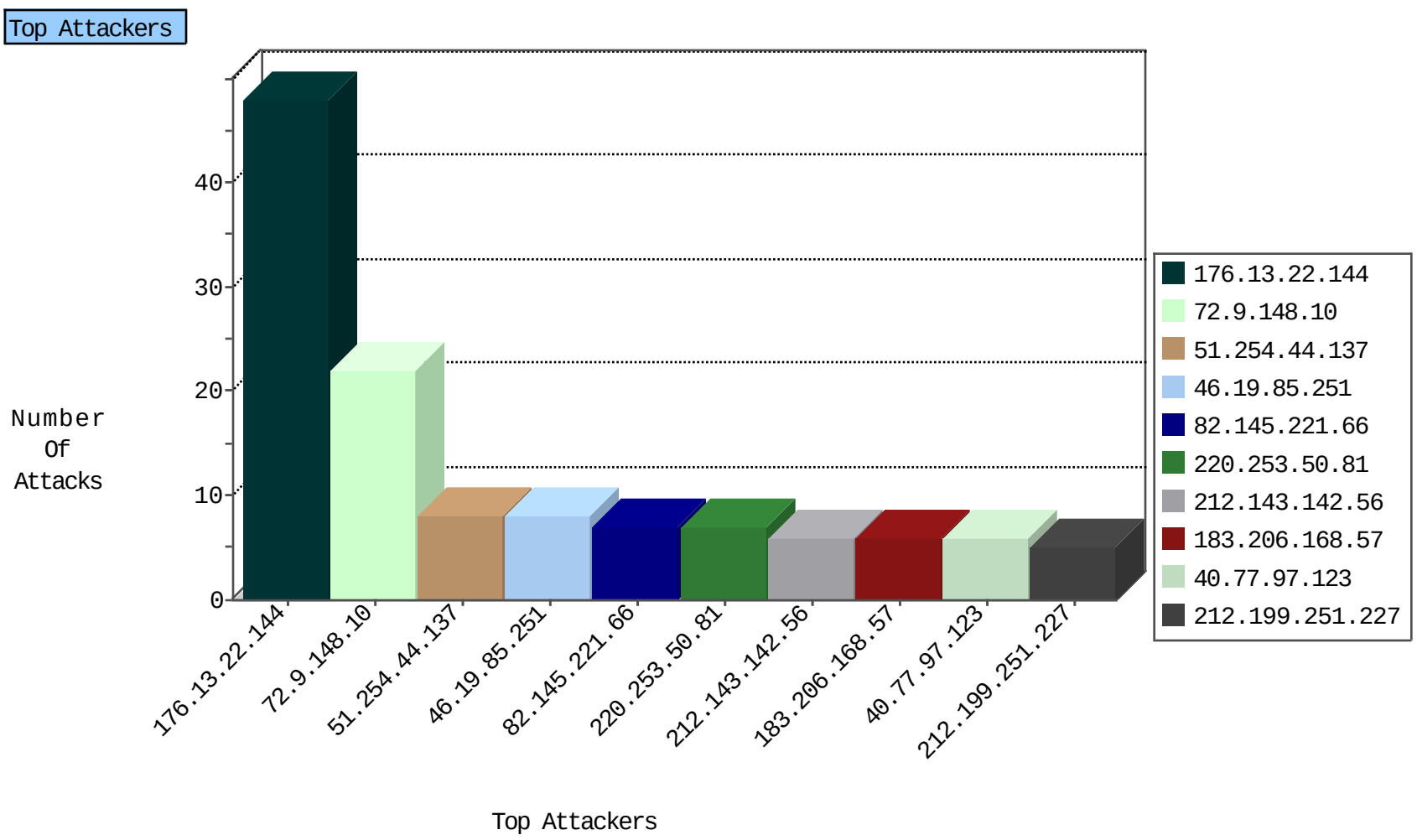
03-08-2016-06:04:01 to 03-08-2016-07:04:01

IDF Under Attack Daily Report





03-08-2016-06:04:01 to 03-08-2016-07:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.221.66	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
119.93.247.4	Philippines	147.237.0.200	m4u.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
184.105.139.84	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
62.75.207.109	Germany	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
66.240.236.119	United States	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.0.34	tikshuv.idf.il	block-sp-traf1	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
198.20.69.98	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.37	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
62.75.207.109	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1

03-08-2016-06:04:01 to 03-08-2016-07:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
178.203.146.227	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
178.203.146.227	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.36	France	147.237.0.15	kosher-kravi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-08-2016-06:04:01 to 03-08-2016-07:04:01

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
91.201.236.113	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
40.77.97.123	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
40.77.97.123	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
40.77.97.123	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.76.148	United States	gqcenter.aka.idf.il	ET DROP Dshield Block Listed Source	1
183.56.166.188	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
40.77.97.123	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
40.77.97.123	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
40.77.97.123	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1

03-08-2016-06:04:01 to 03-08-2016-07:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
46.19.85.251	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
164.138.112.96	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.141.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.250.217.21	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
212.199.251.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.117.57.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
220.253.50.81	Australia	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.236	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
24.24.223.241	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
212.199.251.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
212.199.251.227	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	2
37.26.147.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.84	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.231	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
159.226.95.66	China	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.50	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
51.254.44.137	United Kingdom	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.199.251.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.94	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
93.172.168.71	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.57.136.75	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
51.254.44.137	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.232	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.56	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
220.253.50.81	Australia	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
212.199.251.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.95	United States	147.237.0.33	idf.il	drop		drop	1
137.116.71.170	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.15	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.123	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
51.254.44.137	United Kingdom	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
198.20.69.98	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
2.54.42.104	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
220.253.50.81	Australia	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
70.198.8.232	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.199.251.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.139.120	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.23	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
220.253.50.81	Australia	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
51.254.44.137	United Kingdom	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.84	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

03-08-2016-06:04:01 to 03-08-2016-07:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.22.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
176.13.22.144	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	18
46.19.85.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
31.210.186.23	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
37.142.64.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.89.217.227		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
183.206.160.57	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 183.206.160.57	Block	2
183.206.168.57	China	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 183.206.168.57	Block	1
149.125.70.175	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
183.206.160.57	China	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/fckeditor/editor/	Block	1
94.230.93.50	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
183.206.168.57	China	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 183.206.168.57	Block	1
68.196.162.2	United States	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 68.196.162.2 (Open Mode)	None	1
185.89.217.229		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
183.206.168.57	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 183.206.168.57	Block	1
94.230.93.63	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
183.206.168.57	China	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 183.206.168.57	Block	1
24.196.156.28	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
68.196.162.2	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
51.254.44.137	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to /	Block	1
212.143.38.222	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
183.206.168.57	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/fckeditor/editor/	Block	1
94.230.93.69	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.11	United States	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/	Block	1
185.82.200.91		147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
24.196.156.28	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
183.206.160.57	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/fckeditor/editor/	Block	1
84.108.237.95	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1
51.254.44.137	United Kingdom	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /	Block	1
212.143.38.222	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
183.206.168.57	China	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/fckeditor/editor/	Block	1
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/61998	Block	1
185.82.200.91		147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
94.230.93.24	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
51.254.44.137	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	1
220.253.50.81	Australia	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

03-08-2016-06:04:01 to 03-08-2016-07:04:01