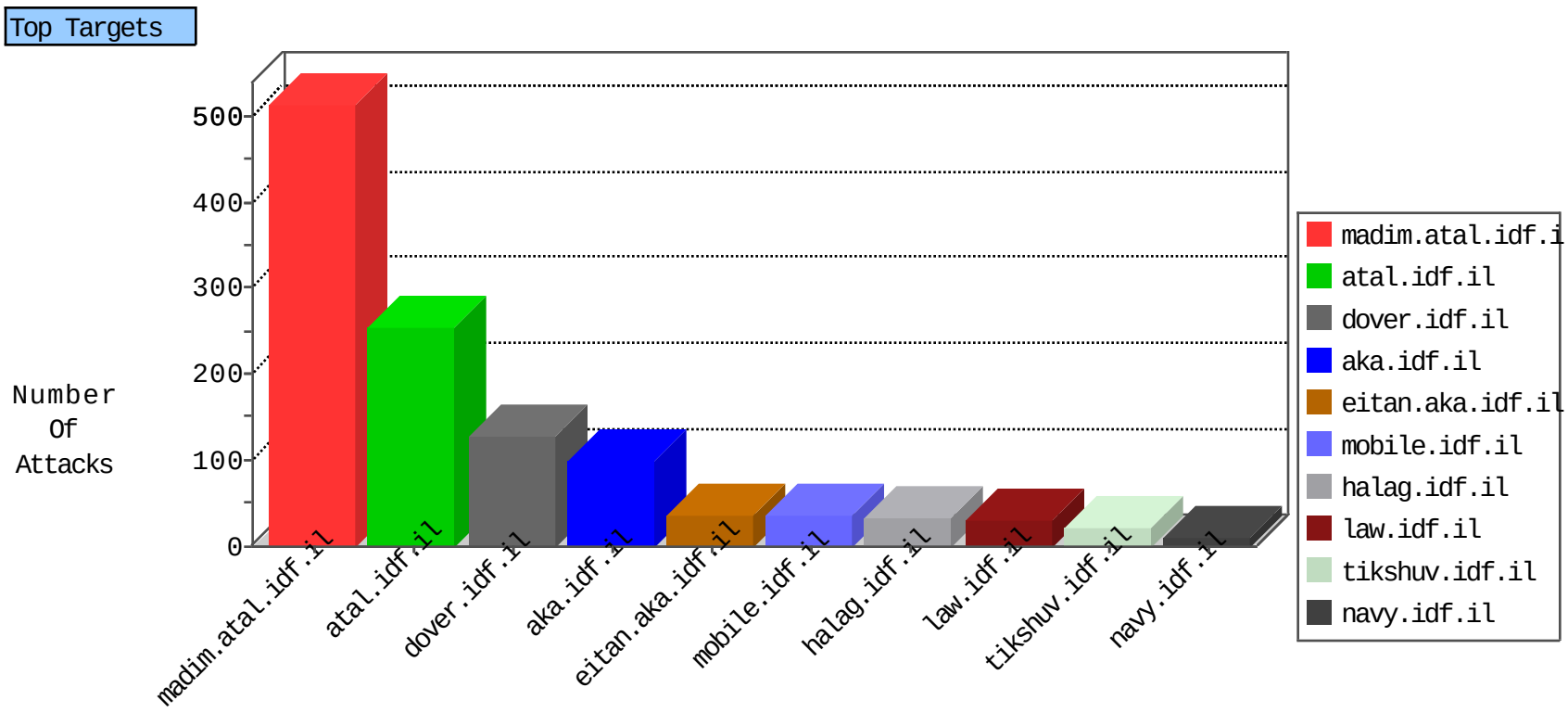
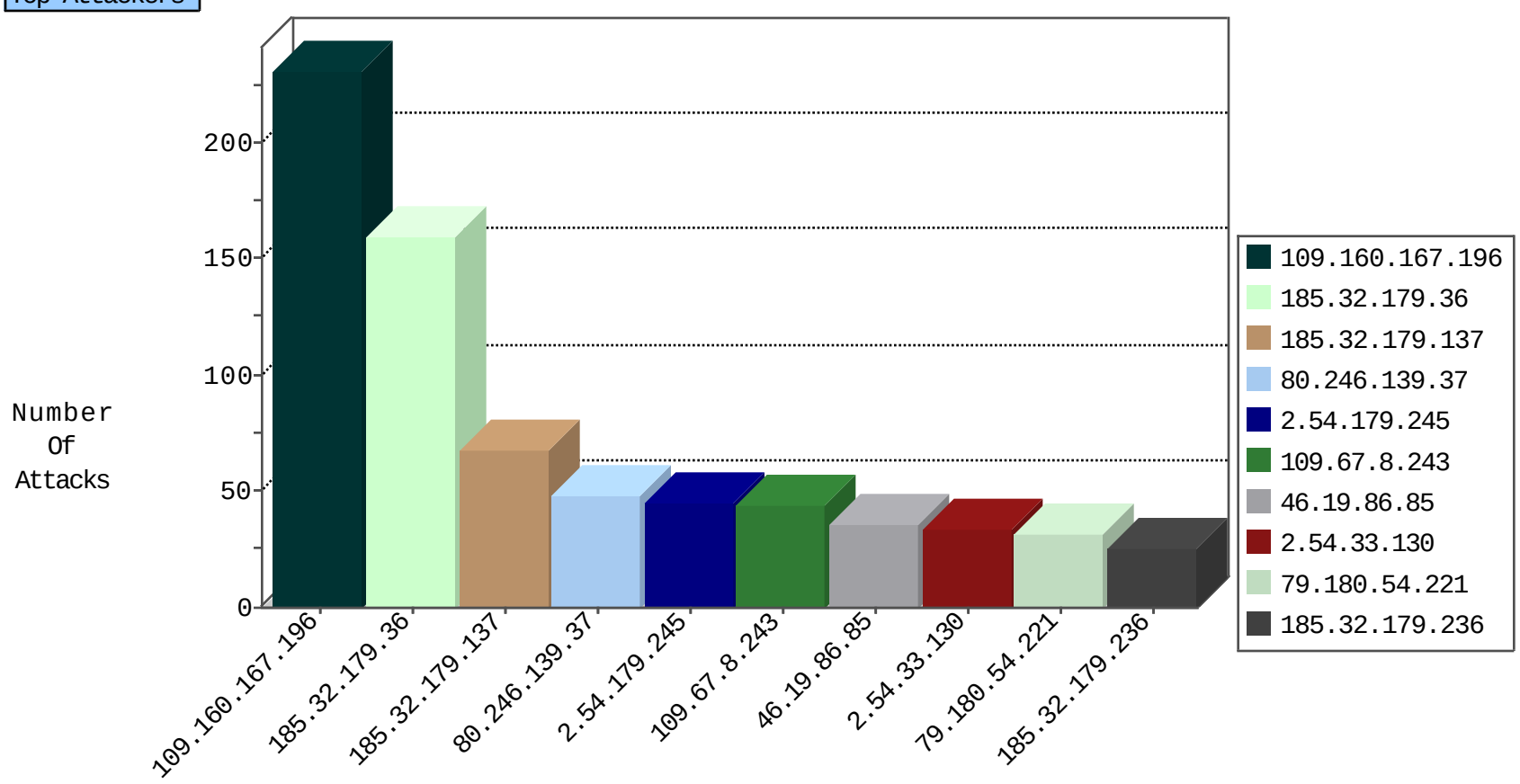
03-06-2016-23:04:00 to 03-07-2016-00:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-06-2016-23:04:00 to 03-07-2016-00:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
141.212.122.211	United States	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
108.186.168.25	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
50.30.37.59	United States	147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1
111.91.157.28	Korea, Republic of	147.237.77.205	prisha.idf.il	Block_Udp_All_Nets	drop	1

03-06-2016-23:04:00 to 03-07-2016-00:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
64.31.44.6	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.8.204.63	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.176.48.200	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
61.135.189.108	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
94.102.153.58	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
46.19.85.125	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
91.121.211.59	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
91.121.211.59	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
149.88.178.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
149.78.174.169	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-06-2016-23:04:00 to 03-07-2016-00:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.102.153.58	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	12
64.31.44.6	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
95.130.13.220	147.237.77.19	France	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
60.212.2.39	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
60.212.2.39	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
185.110.132.54	147.237.77.179		e.mazi.idf.il	ET SCAN Potential SSH Scan	1
185.32.179.36	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
104.128.144.131	147.237.76.30	Canada	himush.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.48.193	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
60.212.2.39	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
60.212.2.39	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.212.202	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

03-06-2016-23:04:00 to 03-07-2016-00:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.160.167.196	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	230
46.19.86.85	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.180.54.221	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
109.253.130.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.237.136.28	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.177.126.167	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.140.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.144.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.16.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.212.202	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.45.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.242.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.212.202	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
111.84.193.29	Thailand	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
79.181.20.142	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
99.60.110.103	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.46.39.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.102.9.93	United States	147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	4
37.46.41.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.102.9.103	United States	147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	4
151.252.97.204	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
149.78.249.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.125.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.123.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.159	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.157.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.64.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	3
5.22.130.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.201.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.119.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.138.95.161	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
149.78.46.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.27.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
123.126.113.154	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.176.201.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.182.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	3
93.157.87.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.183.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-06-2016-23:04:00 to 03-07-2016-00:04:00

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
77.125.83.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
213.57.91.199	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	3
46.19.85.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	2
46.19.86.15	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	159
185.32.179.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
80.246.139.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
109.67.8.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
2.54.179.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
2.54.33.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
185.32.179.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
185.32.179.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
185.32.179.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
185.32.179.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
185.32.179.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
185.32.179.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
45.35.105.129		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
95.86.82.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.126.235.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.160.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
199.30.24.135	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	2
2.54.148.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
131.253.25.220	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
82.80.30.220	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 82.80.30.220	Block	1
185.120.126.73		147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
65.55.210.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.65.103.213	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
79.177.126.167	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.32.179.137	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.148.236	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
132.72.229.215	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 132.72.229.215 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
84.109.148.41	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.64.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/70005.doc	Block	1
197.37.161.186	Egypt	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
109.65.103.213	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
79.180.54.221	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
37.236.8.107	Iraq	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.236.8.107	Block	1
173.247.228.10	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
86.147.154.194	United Kingdom	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.230	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20063-he/idfgdover.aspx	Block	1
197.37.161.186	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
5.29.193.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
79.181.20.142	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
2.54.140.26	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
173.247.228.10	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
109.160.167.196	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
46.19.85.175	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
101.226.167.241	China	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.148.198	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 37.26.148.198 (Open Mode)	None	1

03-06-2016-23:04:00 to 03-07-2016-00:04:00