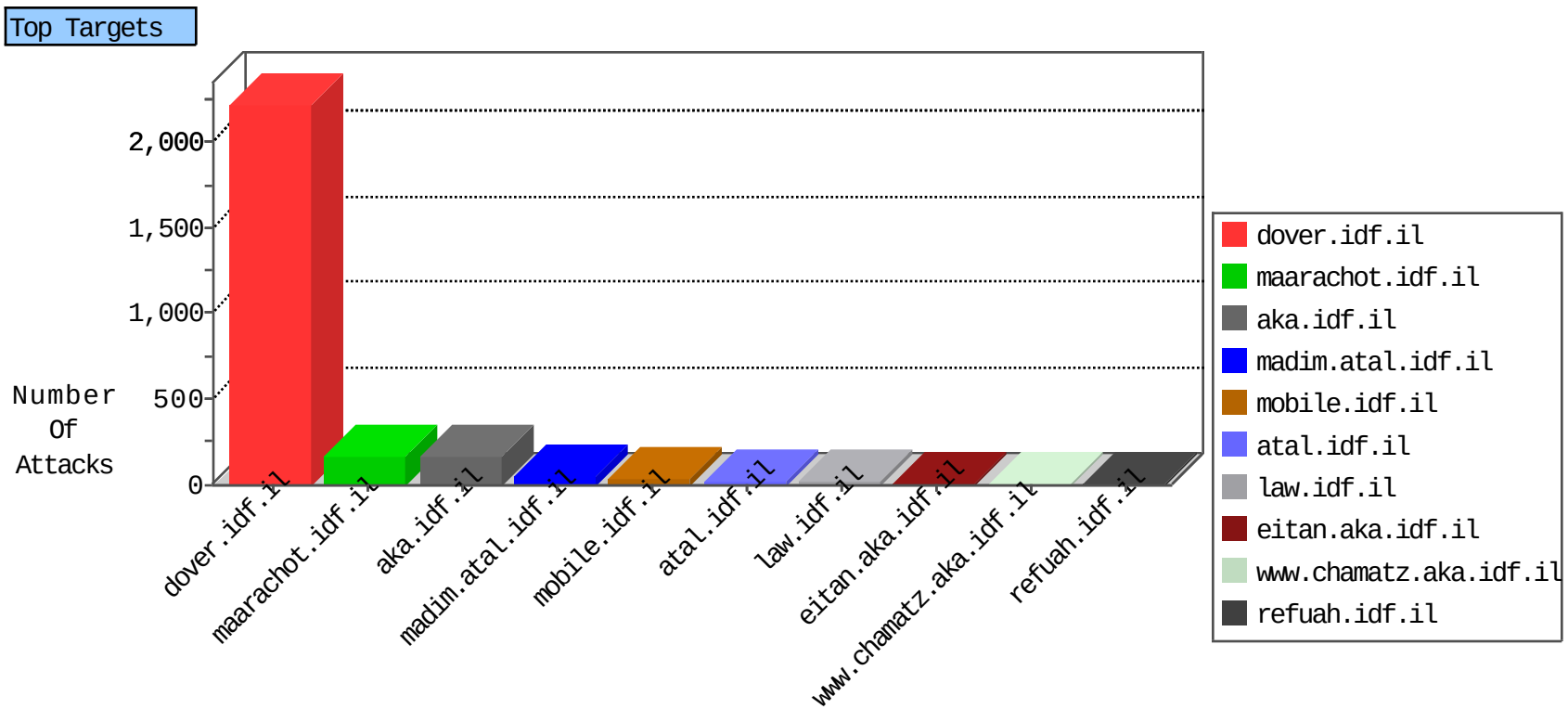
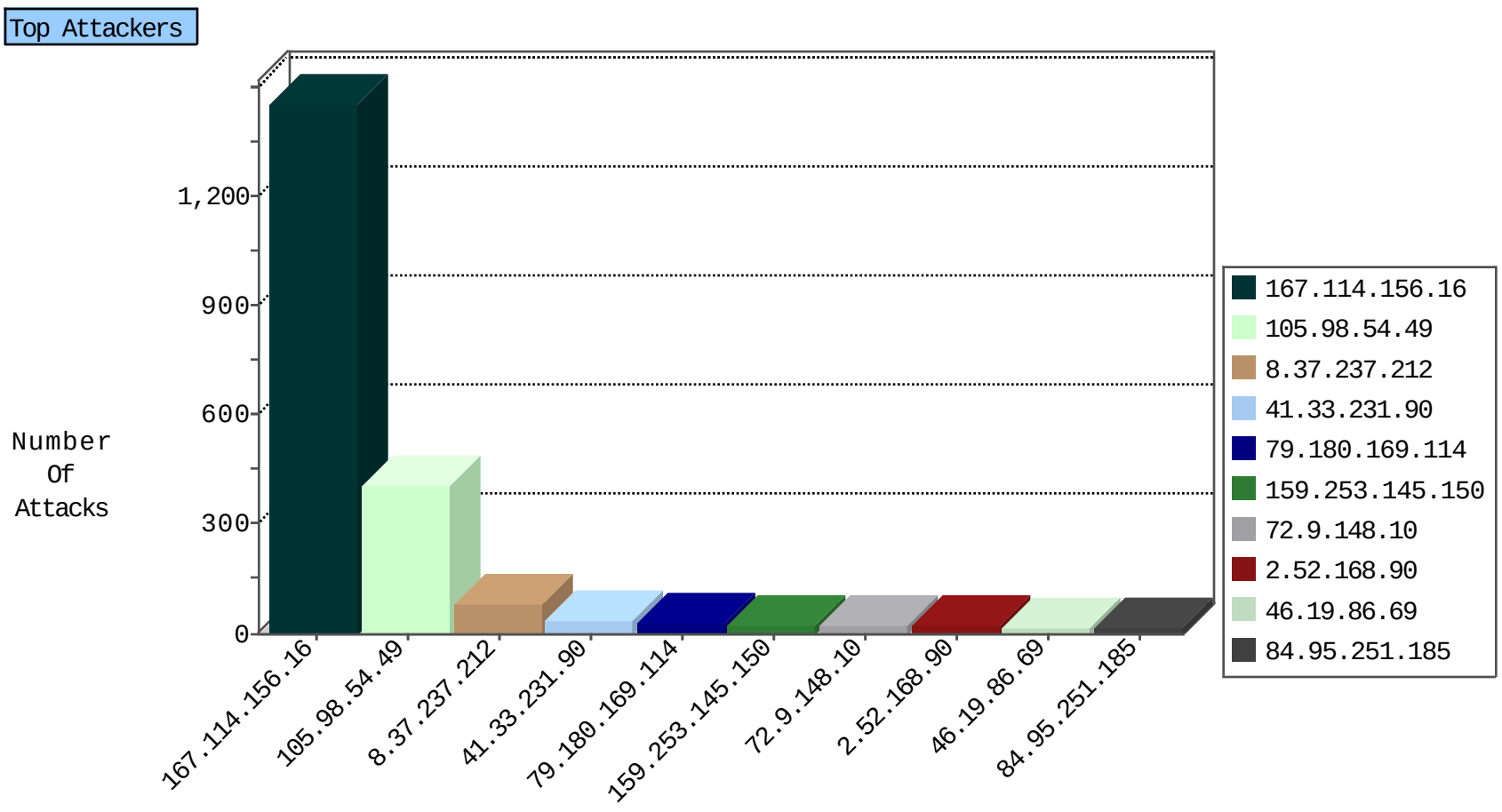
01-02-2016-13:04:04 to 01-02-2016-14:04:04

IDF Under Attack Daily Report



Top Target



Top Attackers

01-02-2016-13:04:04 to 01-02-2016-14:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.98.54.49	Algeria	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	3804
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3135
8.37.71.9	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
8.37.71.39	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
8.37.237.212	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
106.75.199.192	China	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

01-02-2016-13:04:04 to 01-02-2016-14:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
159.253.145.150	United States	147.237.77.216	dover.idf.il	C095: Suspicious Addresses MFA	Permit	25
185.130.5.224		147.237.77.205	prisha.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
151.80.44.115	Italy	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
185.130.5.224		147.237.77.216	dover.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
185.130.5.224		147.237.77.226	www.chamatz.aka.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
185.130.5.224		147.237.77.19	law-forum.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
185.130.5.224		147.237.77.74	law.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-02-2016-13:04:04 to 01-02-2016-14:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
105.98.54.49	147.237.77.216	Algeria	dover.idf.il	ET SCAN NMAP -sS window 1024	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
124.65.196.195	147.237.76.196	China	e.sviva.idf.il	GPL SCAN nmap TCP	2
106.120.201.115	147.237.76.196	China	e.sviva.idf.il	GPL SCAN nmap TCP	2
66.249.66.63	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
223.72.232.242	147.237.76.196	China	e.sviva.idf.il	GPL SCAN nmap TCP	2
209.105.232.241	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.8.46	Cote D'Ivoire	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
103.31.80.226	147.237.76.202	Pakistan	e.halag.idf.il	ET SCAN Potential SSH Scan	1
192.186.95.178	147.237.0.35	Canada	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
103.31.80.226	147.237.76.199	Pakistan	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
174.142.97.6	147.237.0.17	Canada	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
103.31.80.226	147.237.76.196	Pakistan	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
162.244.26.138	147.237.8.24	Canada	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
103.31.80.226	147.237.76.147	Pakistan	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
84.117.113.152	147.237.72.167	Romania	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
124.65.231.114	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
123.20.32.84	147.237.77.19	Vietnam	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
196.47.173.21	147.237.8.46	Cote D'Ivoire	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
103.31.80.226	147.237.76.201	Pakistan	e.atal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.224	147.237.0.200		m4u.idf.il	ET SCAN NMAP -sS window 1024	1
103.31.80.226	147.237.76.197	Pakistan	e.himush.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
103.31.80.226	147.237.76.177	Pakistan	ncore.idf.il	ET SCAN Potential SSH Scan	1
162.244.26.138	147.237.8.24	Canada	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
84.117.113.152	147.237.72.217	Romania	e.idf.il	ET SCAN NMAP -sS window 1024	1
124.65.231.114	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
81.214.135.237	147.237.8.28	Turkey	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
124.65.231.114	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

01-02-2016-13:04:04 to 01-02-2016-14:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.237.212	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	77
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
84.95.251.185	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
109.67.136.122	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
79.180.2.75	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
41.129.228.89	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
217.132.23.73	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
87.69.143.46	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
109.65.14.227	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
79.180.169.114	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
79.176.105.252	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
79.176.114.184	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
80.246.136.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
105.98.54.49	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.180.201.225	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
5.29.138.215	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
46.19.85.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.106.41.74	Palestinian Territory, Occupied	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
109.186.90.116	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.183.168.42	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
79.180.169.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
2.52.168.90	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	6
109.64.80.167	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
101.212.69.108	India	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.34.12.97	Jordan	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
2.52.168.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	5
109.64.80.167	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
176.13.23.154	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.172	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
79.176.213.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.23.154	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.102.254.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.81.174	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
31.154.3.222	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.19.85.174	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.142.68.119	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.81.182	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
2.52.168.90	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
109.64.219.13	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4

01-02-2016-13:04:04 to 01-02-2016-14:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
37.142.200.162	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	7
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	4
2.52.169.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
79.182.49.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.121.102.202	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
5.29.195.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.57.49.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.42.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.177.60.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
217.132.119.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.23.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.88.14.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.186.188.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
132.74.30.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.22.130.139	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/589-he/patzar.aspx=	Block	2
109.253.158.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.39.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.46.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.139.57.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
40.77.167.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19405-he/dover.aspx)	Block	1
79.176.179.19	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.66.39.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1401-he/atal.aspx	Block	1
84.228.222.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.179.6.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.162	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
176.12.147.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.222.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
77.125.79.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
2.54.139.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.230.95.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/maim/kapatz	Block	1
46.166.190.174	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.183.62.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.76	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
5.197.61.161	Azerbaijan	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
109.66.171.110	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.66.171.110	Block	1
66.249.66.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
85.64.250.176	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/7/size338x0/1877.jpg	Block	1
79.179.111.250	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
46.19.85.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/headerupper/	Block	1

01-02-2016-13:04:04 to 01-02-2016-14:04:04