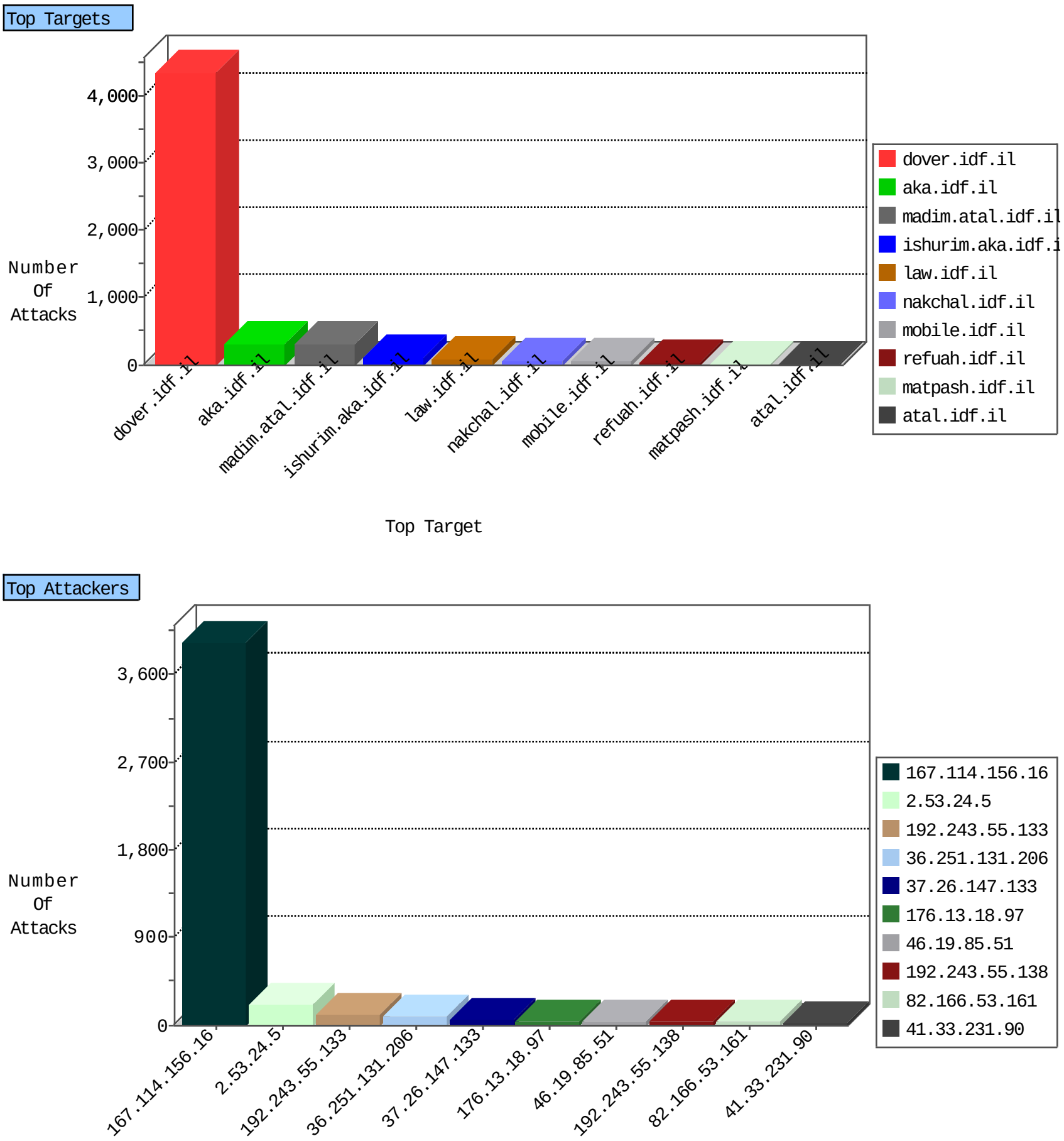
04-11-2016-15:04:05 to 04-11-2016-16:04:05

IDF Under Attack Daily Report



04-11-2016-15:04:05 to 04-11-2016-16:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3937
80.179.69.252	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	13
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
79.181.209.234	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
141.0.14.192	Europe	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
192.118.132.185	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
31.168.133.226	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
192.118.132.185	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
193.43.245.250	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
79.176.132.250	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
179.43.144.50	Switzerland	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
176.31.60.249	France	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
79.181.209.234	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
176.31.60.249	France	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
62.138.2.122	Germany	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
179.43.141.194	Switzerland	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1

04-11-2016-15:04:05 to 04-11-2016-16:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.150	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
144.76.93.46	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
144.76.93.46	Germany	147.237.76.147	chinuch.aka.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
144.76.93.46	Germany	147.237.77.226	www.chamatz.aka.idf.il	C1000074: HTTP: majestic bot	Block	2
85.64.109.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
144.76.93.46	Germany	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Block	1
61.135.189.122	China	147.237.76.31	nakchal.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

04-11-2016-15:04:05 to 04-11-2016-16:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
208.100.26.228	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
192.243.55.133	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.215.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.1.189	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.104.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
13.92.245.177	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
188.3.34.20	147.237.0.33	Turkey	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
87.70.115.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.156.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.238	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-11-2016-15:04:05 to 04-11-2016-16:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.18.97	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
82.166.53.161	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	28
109.65.123.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
82.166.221.34	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	24
176.13.4.50	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	18
192.243.55.133	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
80.246.133.91	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
2.52.161.166	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.117.167.66	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
109.64.57.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
87.71.97.177	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
37.142.68.36	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
192.243.55.133	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
82.166.53.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.133	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.147.133	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
64.113.191.31	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.147.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
46.19.85.214	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.7.25	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.133	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.150.218.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.133	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	6
79.181.174.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.214	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.80.86.50	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.147.133	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.133	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.115.133.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.197	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence		alert	6
37.26.147.133	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
37.26.147.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.147.197	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence		monitor	6
37.26.147.133	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
95.35.191.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.133	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.138	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4

04-11-2016-15:04:05 to 04-11-2016-16:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.24.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	218
36.251.131.206	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 36.251.131.206	Block	69
46.19.85.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
36.251.131.206	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	14
147.236.38.135	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	13
176.13.22.94	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	12
46.19.86.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
212.117.143.250	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	9
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.55.55.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
147.236.38.135	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 147.236.38.135	Block	3
109.253.205.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.38.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.117.143.250	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/7/	Block	2
37.26.148.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
65.55.210.205	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
192.243.55.133	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	2
212.179.21.194	Israel	147.237.77.176	matpash.idf.il	Distributed Abnormally Long Request	Block	2
2.52.166.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.166.53.78	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.179.21.194	Israel	147.237.77.176	matpash.idf.il	Distributed Unknown HTTP Request Method	Block	2
176.13.4.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.106.96.91	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	2
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Illegal Byte Code Character in URL ™9˙an:פ•,d†	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
65.55.210.140	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Method	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/general	Block	1
97.83.188.239	United States	147.237.76.42	refuah.idf.il	NULL Character in Method	Block	1
79.178.108.173	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
176.13.4.236	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.220.145.245	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	NULL Character in URL	Block	1
46.218.24.119	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/chinuch.aspx	Block	1
87.71.179.7	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Malformed URL ™9˙an:פ•,d†	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
105.157.194.123	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
80.246.133.91	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
31.168.103.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/shared/warn_icon.png	Block	1
176.13.7.25	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Abnormally Long Request method	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
54.88.169.180	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il./robots.txt	Block	1
37.142.68.36	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
192.118.78.57	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/rules.abe	Block	1
93.172.30.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method [[#24]]•Í¨âè[[#18]]uË[[#24]]p1çr2WO[[#15]]zËŠú#"ij1©lí[[#29]]'[[#26]]›Q1%q in URL ™9˙an:Ð•,d†	Block	1

04-11-2016-15:04:05 to 04-11-2016-16:04:05