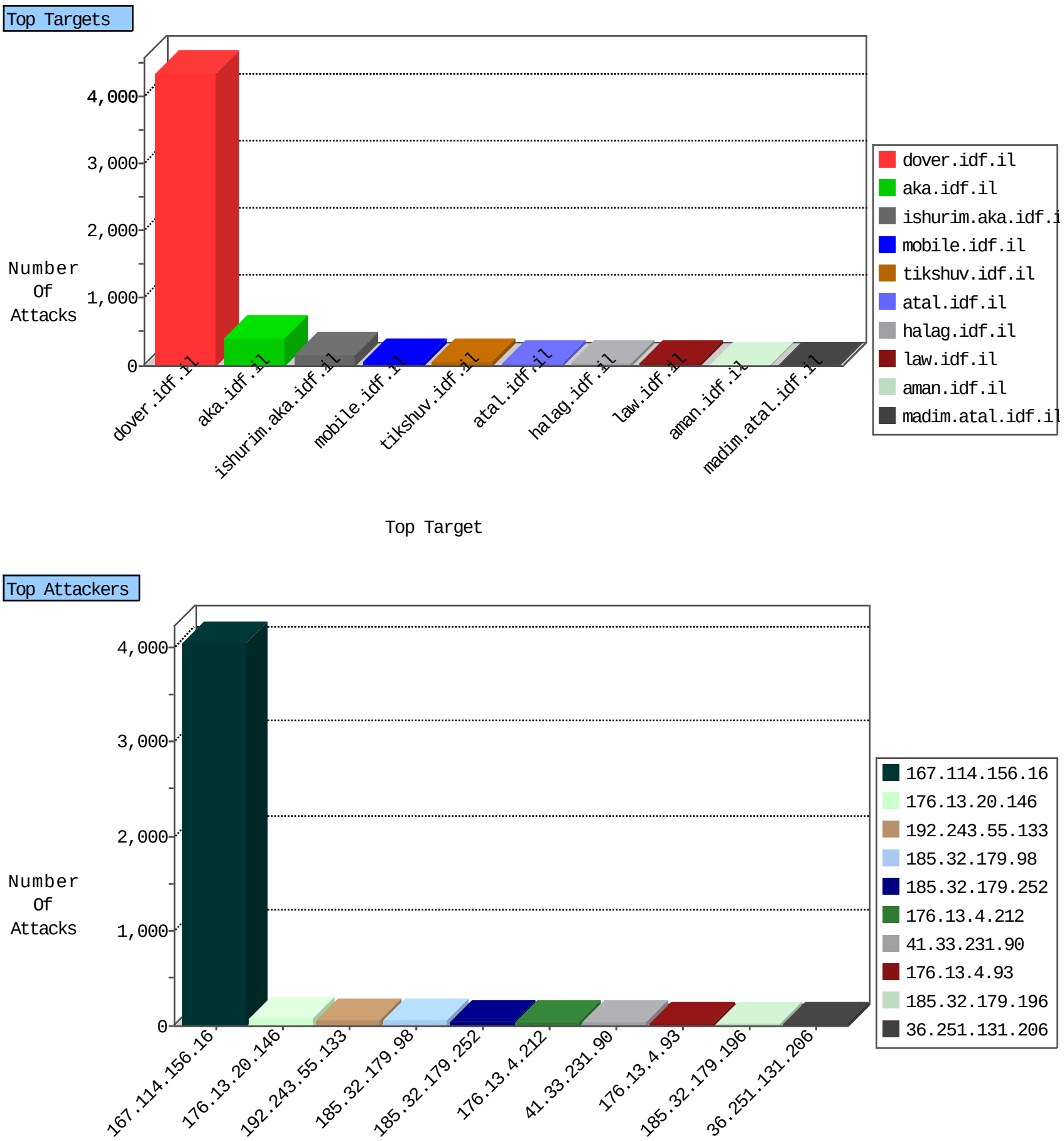
04-11-2016-16:04:08 to 04-11-2016-17:04:08

IDF Under Attack Daily Report



04-11-2016-16:04:08 to 04-11-2016-17:04:08

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	4039
82.145.219.172	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
179.43.141.194	Switzerland	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
209.126.110.228	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
124.205.27.162	China	147.237.76.202	e.halag.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
212.179.219.26	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
62.138.2.122	Germany	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1

04-11-2016-16:04:08 to 04-11-2016-17:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.28.173.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
62.90.88.104	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.19.86.158	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
213.151.51.210	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
106.38.241.150	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
46.19.86.220	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
192.116.92.53	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.93.109	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.178.216.248	Israel	147.237.77.170	maarachot.idf.il	C1000008: HTTP: Xenu UserAgent	Block	2
87.69.154.116	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
147.234.241.18	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
66.249.93.101	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	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
62.90.99.43	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.93.97	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-11-2016-16:04:08 to 04-11-2016-17:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.117.208.243	147.237.77.243		mobile.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.28.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
203.197.205.118	147.237.76.31	India	nakchal.idf.i	ET SCAN NMAP -sS window 4096	1
80.82.78.38	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
203.197.205.118	147.237.76.31	India	nakchal.idf.i	ET SCAN NMAP -f -sS	1
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
168.235.85.68	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.27	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.64.31.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.254.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.113.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.161.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.232.98.3	147.237.76.196	United States	e.sviva.idf.i	ET SCAN NMAP -sS window 1024	1
84.240.57.96	147.237.77.216	Lithuania	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.175.105	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.76.105.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.38	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
203.197.205.118	147.237.76.31	India	nakchal.idf.i	ET SCAN NMAP -sS window 2048	1
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
46.116.240.13	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.22.249	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.221.102	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.172.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.164.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
106.77.16.82	147.237.77.243	India	mobile.idf.il	GPL SCAN nmap TCP	1
87.71.92.225	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

04-11-2016-16:04:08 to 04-11-2016-17:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.20.146	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
176.13.4.212	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
31.154.144.67	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
46.19.85.217	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
2.54.172.162	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
100.127.5.50		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
185.32.179.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	18
193.191.219.80	Belgium	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	13
185.32.179.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	12
46.19.86.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.108	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.32.179.98	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
185.32.179.98	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
79.181.208.228	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
185.32.179.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	10
192.114.91.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
37.26.148.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.32.179.252	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
185.32.179.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.60	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.20.146	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
185.32.179.252	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
185.32.179.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
185.32.179.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
185.32.179.196	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
185.32.179.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.133	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
185.32.179.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.219.128.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.193	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.141.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.164	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.228.10.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.147.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.14.44	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.179.118.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.71.99.17	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.15	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.186	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
185.32.179.196	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.60	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.54.160.93	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.20.146	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
36.251.131.206	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 36.251.131.206	Block	25
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
2.54.132.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
173.236.187.27	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 173.236.187.27	Block	5
36.251.131.206	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	5
176.13.4.93	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 176.13.4.93	Block	4
176.13.4.93	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 176.13.4.93	Block	4
46.19.85.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
66.102.7.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.19.85.217	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.13.4.93	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 176.13.4.93	Block	4
46.19.86.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.4.93	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 176.13.4.93	Block	3
176.13.8.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.4.93	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 176.13.4.93	Block	3
185.27.106.47	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/hinuch	Block	2
46.19.85.15	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
185.27.106.47	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.27.106.47	Block	2
46.19.85.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.117.3.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	2
80.246.130.31	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.7	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.13.4.93	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 176.13.4.93	Block	2
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.246.130.126	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
176.13.4.93	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 176.13.4.93	Block	1
65.208.151.115	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	1
199.30.25.141	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.4.93	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version òQÛˆS1[[#25]][[#5]]tŸô[[#19]]™â‰•ê[[#11]]¤½×[[#17]]	Block	1
157.55.2.134	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.89.217.224	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.1.106.195	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/favicon.ico	Block	1
176.13.4.93	Israel	147.237.72.166	aka.idf.il	NULL Character in URL ¸[[#28]]Xr[[#0]]p[[.•#31(aj‹÷•„±\]]′	Block	1
68.180.230.187	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation PageNum in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1232-he/atal.aspx	Block	1
46.19.86.246	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	1
173.236.187.27	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
80.246.133.136	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/scriptresource.axd	Block	1
176.13.4.93	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 1	Block	1
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
157.55.12.92	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.89.217.229	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
8.37.232.37	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.4.93	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
72.238.75.87	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
66.249.66.29	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1