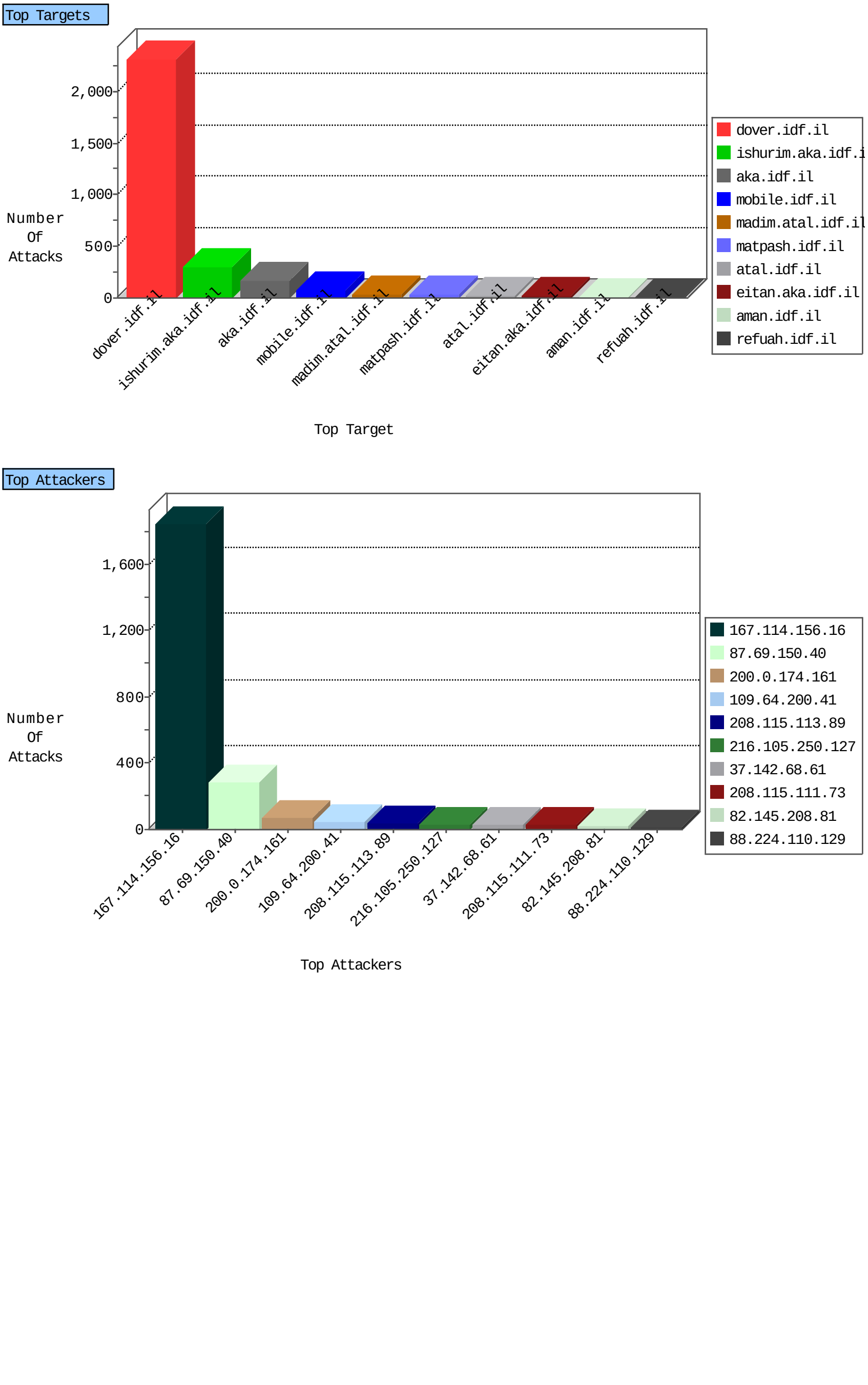
04-26-2016-16:04:08 to 04-26-2016-17:04:08

IDF Under Attack Daily Report



04-26-2016-16:04:08 to 04-26-2016-17:04:08

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	HTTP-POST-Segmented-DoS	dest-reset	9626
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	6996
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	229
109.67.203.188	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	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
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
94.102.49.116	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
66.240.236.119	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
71.6.158.166	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
113.119.217.95	China	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
31.148.219.11	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
134.134.139.74	United States	147.237.77.176	matpash.idf.il	Frk_Under_Attack_Con_Http	drop	1

04-26-2016-16:04:08 to 04-26-2016-17:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.74.38.14	Sweden	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

04-26-2016-16:04:08 to 04-26-2016-17:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.74.38.14	147.237.77.233	Sweden	atal.idf.il	SQL Injection - Select From	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
183.60.48.25	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
93.174.95.73	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
76.181.249.213	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	147.237.77.74	Turkey	law.idf.il	ET SCAN NMAP -sS window 1024	1
76.181.249.213	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1

04-26-2016-16:04:08 to 04-26-2016-17:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1545
87.69.150.40	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	282
200.0.174.161	Chile	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
109.64.200.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
216.105.250.127	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
82.145.208.81	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
97.74.24.187	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.133.45	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
107.170.186.68	United States	147.237.77.176	matpash.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	11
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
88.224.110.129	Turkey	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	7
88.224.110.129	Turkey	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
176.13.16.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
98.248.47.127	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.146.217	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.146.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.23.94	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
207.46.13.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
128.90.88.239	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.102.242.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
157.55.39.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
89.138.253.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.102.195.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.111	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
188.120.154.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
173.240.233.254	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.107.109.226	Saudi Arabia	147.237.77.216	dover.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
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.43.209.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
108.166.28.136	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
95.211.70.193	Netherlands	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
31.210.187.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.74.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.0.169	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
87.145.195.11	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

04-26-2016-16:04:08 to 04-26-2016-17:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.68.61	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.142.68.61	Block	26
109.253.136.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.253.145.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.65.208.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
85.65.225.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.150.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
38.111.147.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
37.26.149.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.182.131.120	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1437-he/atal.aspx	Block	2
207.241.226.231	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
5.102.254.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.170.186.68	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 107.170.186.68	Block	2
176.13.19.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.253	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
82.80.132.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
212.150.163.132	Israel	147.237.76.42	refuah.idf.il	NULL Character in Method	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1956-he/cogat.aspx	Block	1
164.132.161.28	Italy	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/rights/hebrew/html	Block	1
109.65.146.101	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
54.237.118.69	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
207.241.226.230	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.55.56.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
175.144.22.182	Malaysia	147.237.77.74	law.idf.il	PHP Attempt	Block	1
37.142.68.61	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/contactus/mobile	Block	1
109.65.146.101	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.65.146.101	Block	1
81.223.254.34	Austria	147.237.77.216	dover.idf.il	Unauthorized URL Access to /robots.txt	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/3347.jpg	Block	1
149.78.72.28	United States	147.237.0.34	tikshuv.idf.il	Automated Vulnerability Scanning V1	Block	1
5.102.147.192	Switzerland	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/tmp/php.class.php	Block	1
93.173.181.158	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
175.144.22.182	Malaysia	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
81.223.254.34	Austria	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /robots.txt	Block	1
66.249.78.130	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/signals/atar/	Block	1
157.55.39.147	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	1
2.53.23.94	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
82.80.129.179	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/71556.pdf	Block	1
212.150.163.132	Israel	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method	Block	1
37.26.146.217	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
107.170.186.68	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
79.178.230.161	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
51.255.65.77	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/smalim/html/11.asp	Block	1
192.114.23.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
2.53.30.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1

04-26-2016-16:04:08 to 04-26-2016-17:04:08