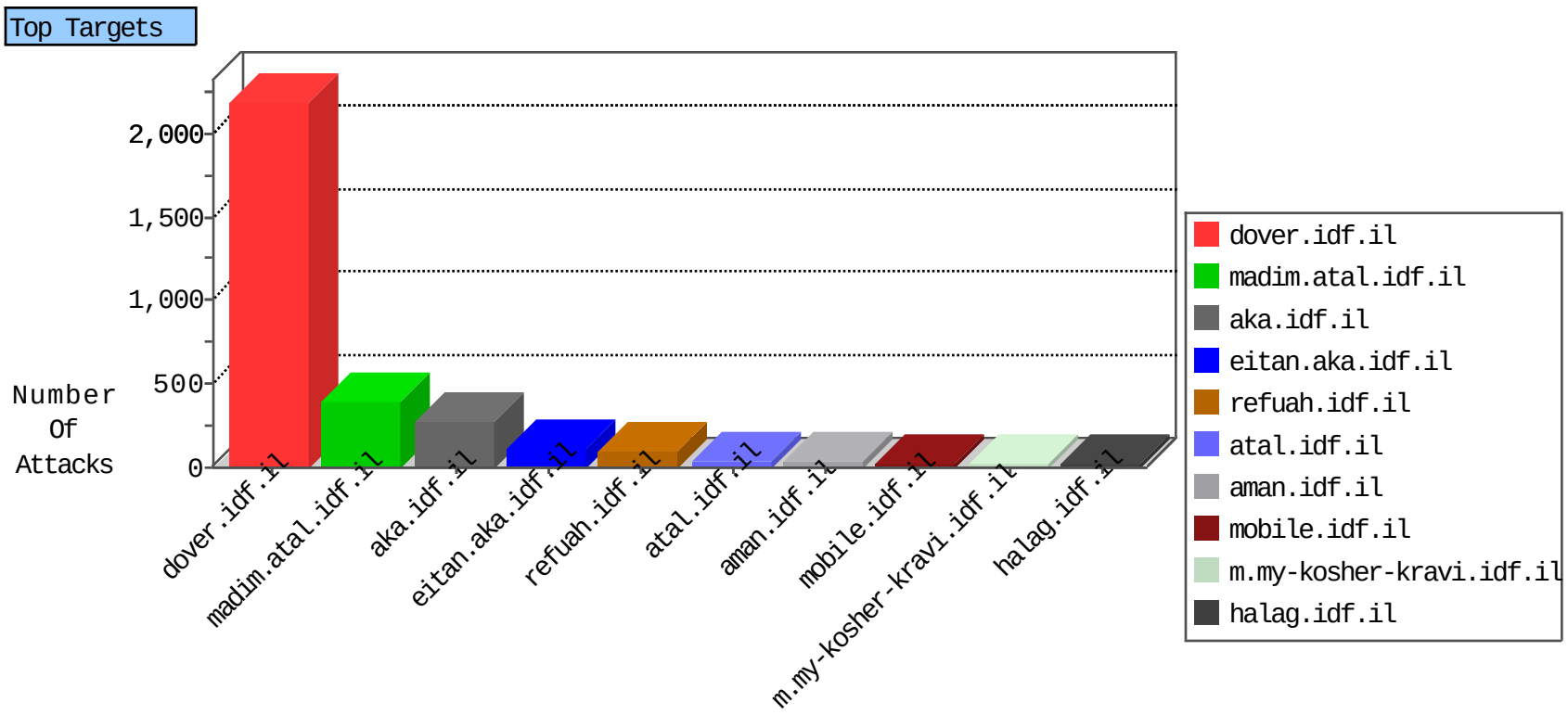
12-26-2015-20:04:00 to 12-26-2015-21:04:00

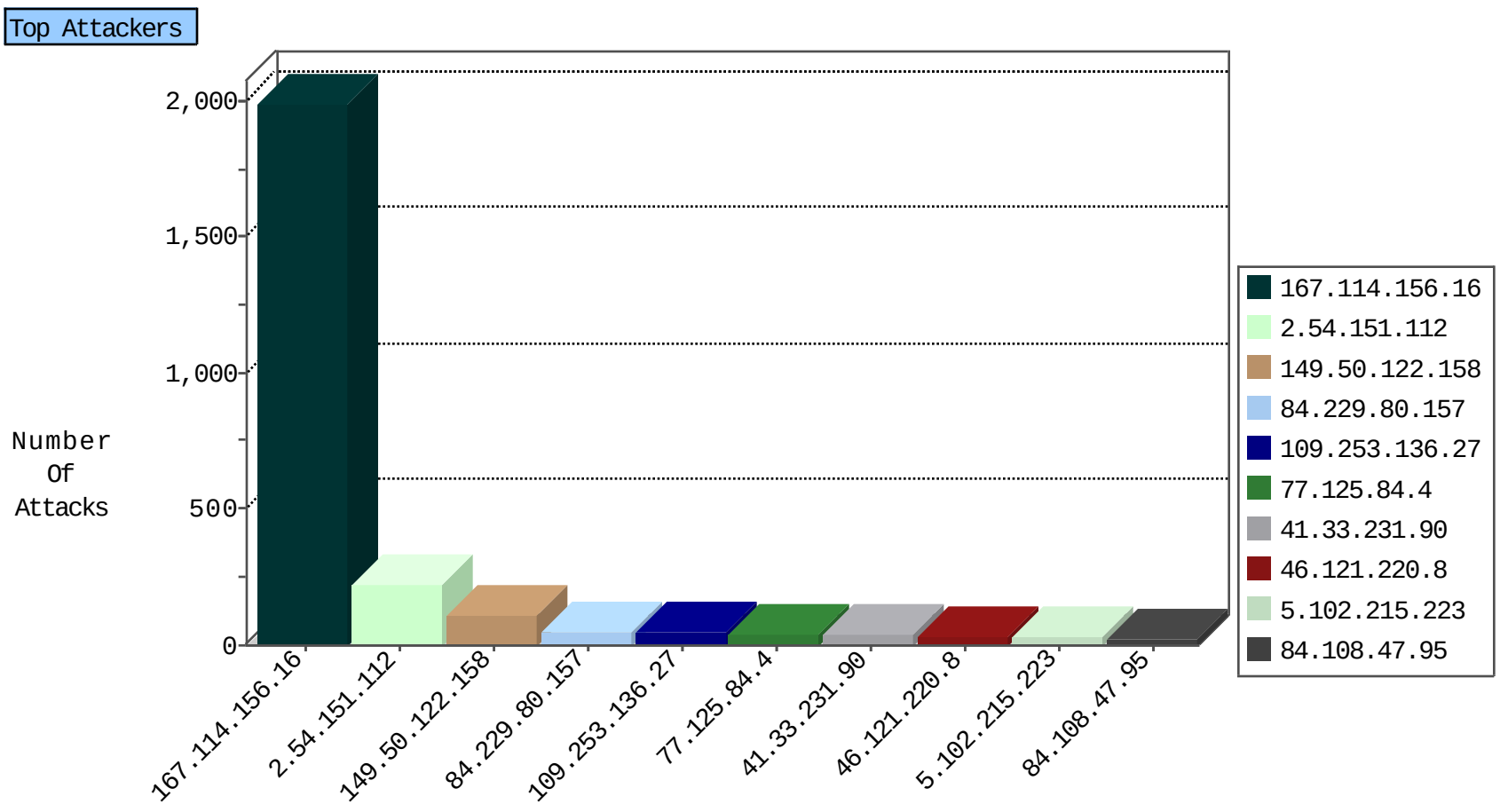
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

12-26-2015-20:04:00 to 12-26-2015-21:04:00

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	DOS-Tool-SwitchbladG	dest-reset	3124
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
95.26.16.196	Russian Federation	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

12-26-2015-20:04:00 to 12-26-2015-21:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.220.8	Israel	147.237.77.233	atal.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	14
88.14.164.68	Spain	147.237.77.176	matpash.idf.il	C008: HTTP: Xenu UserAgent	Block	2

12-26-2015-20:04:00 to 12-26-2015-21:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.81.202	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.191	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
189.254.90.133	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
91.208.115.34	147.237.0.33	Ukraine	idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.172	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
221.226.31.210	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
43.229.53.89	147.237.0.34	Japan	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
221.6.32.82	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.76.176	United States	test.ncore.idf.il	ET DROP Dshield Block Listed Source	1
59.45.79.117	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
189.254.90.133	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.126	147.237.8.27	Netherlands	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
43.229.53.89	147.237.0.35	Japan	akaws.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
221.226.31.210	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
221.6.32.82	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -f -sS	1

12-26-2015-20:04:00 to 12-26-2015-21:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.229.80.157	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
77.125.84.4	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
149.50.122.158	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
5.22.129.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.183.218.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.98	Israel	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
149.88.156.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.28.150.20	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
185.32.179.225	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
77.126.144.25	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.207.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.103	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
31.154.164.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.251.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.207.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.121.220.8	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.52.21.71	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
31.168.30.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.33.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.254.62	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
94.230.80.189	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.13.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.103	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
94.230.86.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.117.113.147	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	5
149.78.101.111	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
31.25.74.132	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
46.117.113.147	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
66.249.83.161	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
176.13.15.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.121.70.195	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.253.137.140	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
95.108.132.178	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
87.68.80.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.0.15.218	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
31.154.163.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.132.102.130	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
82.80.148.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.52.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.131	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.127.55.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
84.108.237.5	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

12-26-2015-20:04:00 to 12-26-2015-21:04:00

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
66.249.93.128	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.151.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
2.54.151.112	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.151.112	Block	108
149.50.122.158	United States	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 149.50.122.158	Block	92
109.253.136.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
5.102.215.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
84.108.47.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
149.88.136.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
2.52.150.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
37.26.146.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
109.253.147.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.121.220.8	Israel	147.237.77.233	atal.idf.il	Unauthorized HTTP Method	Block	5
46.121.220.8	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/sip_storage/files/8/2828.jpg	Block	5
87.69.87.39	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation __EVENTVALIDATION in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	4
128.127.107.123	Netherlands	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.19.86.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.21.201	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 79.177.21.201	Block	3
46.19.85.98	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Byte Code Character in Parameter Value from 46.19.85.98	Block	3
213.57.49.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.247.30.234	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	2
149.78.23.186	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/6/size338x0/1806.jpg	Block	2
77.125.163.231	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
79.177.122.43	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
79.183.62.16	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
80.246.139.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
78.47.17.5	Germany	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
176.13.16.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
5.29.104.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.75.77.119	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/28/	Block	1
149.88.241.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.98	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.19.85.98	None	1
87.69.135.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.93.111.60	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
41.204.202.31	South Africa	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
81.218.202.150	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 81.218.202.150	Block	1
197.85.182.58	South Africa	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.66.39	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
128.73.94.197	Russian Federation	147.237.76.86	navy.idf.il	Suspicious Response Code	Block	1
31.8.161.150	Russian Federation	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	1
79.177.97.111	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
187.189.195.40	Mexico	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/a2billing/customer/iridium_threed.php	Block	1
50.63.85.245	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
109.67.118.39	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.173.231.46	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 10.100.102.8/upnpcp/notify/event	Block	1
217.132.102.130	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
77.232.164.159	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation id in www.idf.il/1294-en/dover.aspx	Block	1
176.12.148.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1