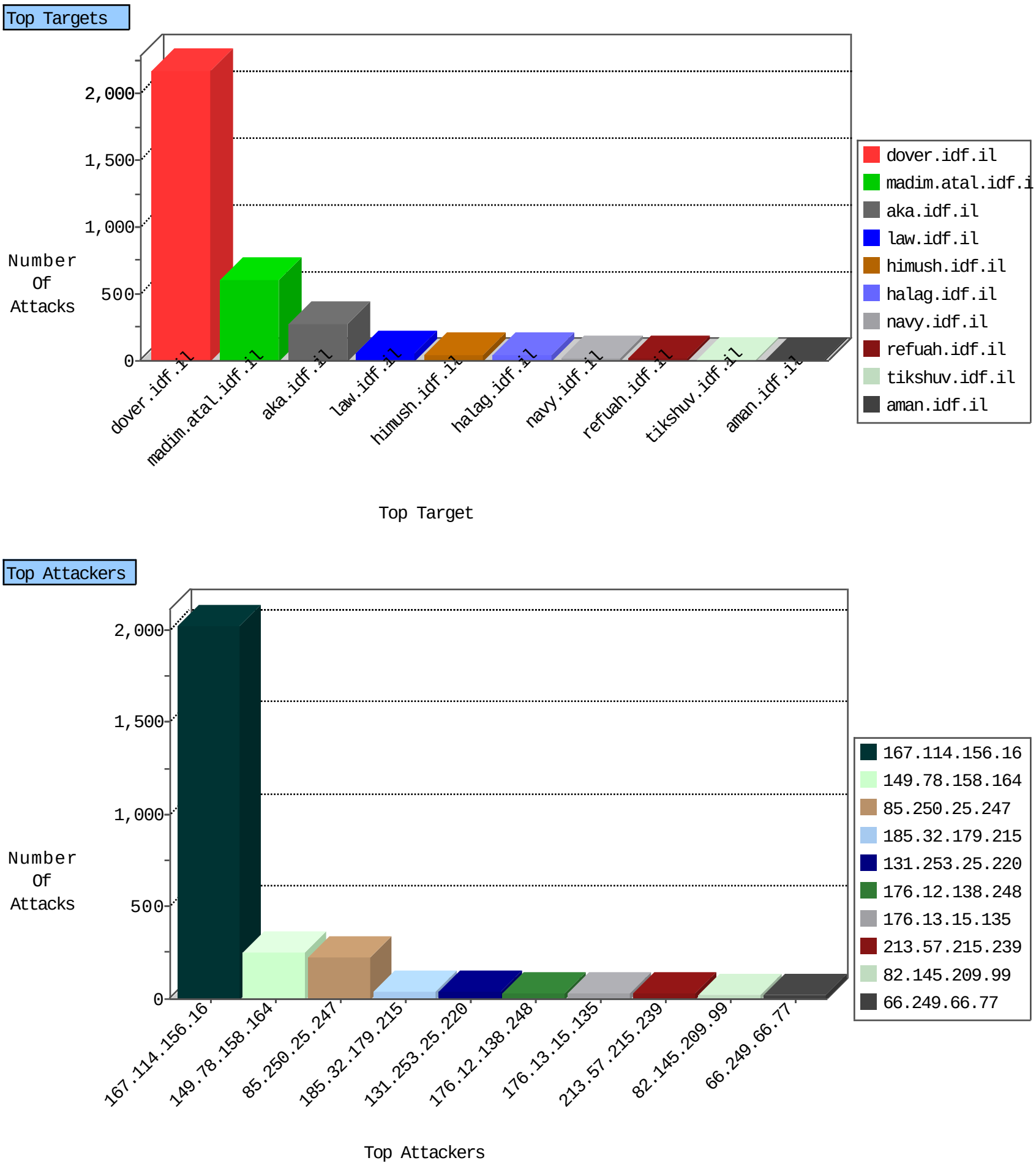
12-16-2015-07:04:05 to 12-16-2015-08:04:05

IDF Under Attack
Daily Report



12-16-2015-07:04:05 to 12-16-2015-08:04:05

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	DOS-Tool-SwitchbladG	dest-reset	3601

12-16-2015-07:04:05 to 12-16-2015-08:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.108.59	Netherlands	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	4
175.126.165.66	Korea, Republic of	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

12-16-2015-07:04:05 to 12-16-2015-08:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
198.20.108.59	147.237.77.216	Netherlands	dover.idf.il	SQL Injection - Select From	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
108.184.162.6	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
198.20.108.59	147.237.77.216	Netherlands	dover.idf.il	GPL WEB_SERVER /etc/passwd	2
175.44.218.6	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
128.199.75.236	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
108.184.162.6	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
108.184.162.6	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
42.118.12.100	147.237.72.217	Vietnam	e.idf.il	ET SCAN NMAP -f -sS	1
5.39.222.253	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
175.44.218.6	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
128.199.254.26	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
108.184.162.6	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
42.118.12.100	147.237.72.217	Vietnam	e.idf.il	ET SCAN NMAP -sS window 2048	1
183.60.48.25	147.237.77.216	China	dover.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

12-16-2015-07:04:05 to 12-16-2015-08:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
131.253.25.220	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
82.145.209.99	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
216.223.27.26	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
46.19.86.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.186.228.93	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.146.171	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	9
216.223.27.30	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
216.223.27.53	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
31.186.228.58	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
31.186.228.32	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
31.186.228.29	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
31.186.228.95	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
31.186.228.30	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
173.252.88.248	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
31.186.228.59	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
94.230.86.145	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.186.228.31	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
31.186.228.60	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
213.57.215.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
68.180.229.239	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.186.228.57	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
213.57.215.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
89.138.2.139	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
213.57.215.239	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
213.57.215.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
66.249.93.13	United States	147.237.76.202	e.halag.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	4
173.252.88.249	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
98.28.144.151	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.215.239	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
173.252.88.251	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
31.186.228.94	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
110.171.186.58	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
173.252.90.117	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.118.11.124	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.182.63.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.13	Israel	147.237.76.202	e.halag.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	3
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.237.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
69.171.228.116	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
192.118.11.124	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.158.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	118
85.250.25.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
149.78.158.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	109
85.250.25.247	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 85.250.25.247	Block	105
185.32.179.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
176.12.138.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
176.13.15.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
149.78.158.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	22
66.249.66.77	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	21
176.13.13.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
80.246.139.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
85.250.25.247	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 85.250.25.247	Block	7
66.249.66.80	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	6
208.115.111.74	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	4
37.26.146.172	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
198.20.108.59	Netherlands	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 198.20.108.59	Block	3
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
185.32.179.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
157.55.39.89	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.20.13	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
82.80.193.244	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
109.64.53.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
84.94.38.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	2
66.215.48.143	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
208.115.113.93	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
37.26.146.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
198.20.108.59	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/nosuchpage123	Block	1
79.176.157.52	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
141.212.122.208	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.75.6	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8928-he/refuah.aspx	Block	1
207.46.13.169	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
46.19.85.94	Israel	147.237.0.34	tikshuv.idf.il	Illegal HTTP Version _pk_id.186.dfb3=19e4e264fcf7592c.1446463637.13.1450244451.1450244451.; _pk_ses.186.dfb3=*	Block	1
2.54.138.178	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20145-he/dover.aspx	Block	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1399-he/atal.aspx	Block	1
213.57.215.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
85.250.25.247	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	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
66.249.75.15	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2799.jpg	Block	1
46.19.85.94	Israel	147.237.0.34	tikshuv.idf.il	Malformed URL _pk_ref.186.dfb3=["","",1450244451,"https://www.google.co.il/"];	Block	1
207.46.13.169	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;sOrderBy in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
87.69.27.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /mivtza>Ñ?Ð¿ÐµÑ†Ð¸Ð°Ð»ÑŒ Ð½Ð¾Ð¼ Ñ?Ð°Ð¹Ñ‚Ðµ, Ñ?Ð¾Ð·Ð´Ð°Ð½Ð½Ð¾Ð¼ Ð´Ð»Ñ? Ñ?Ñ‚Ð¸Ñ… Ñ†ÐµÐ»ÐµÐ¹.</p></div> </div> <table cellspacing=	Block	1
185.120.125.25		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.221	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16775-en/dover.aspx-title=chief	Block	1
85.250.25.247	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1