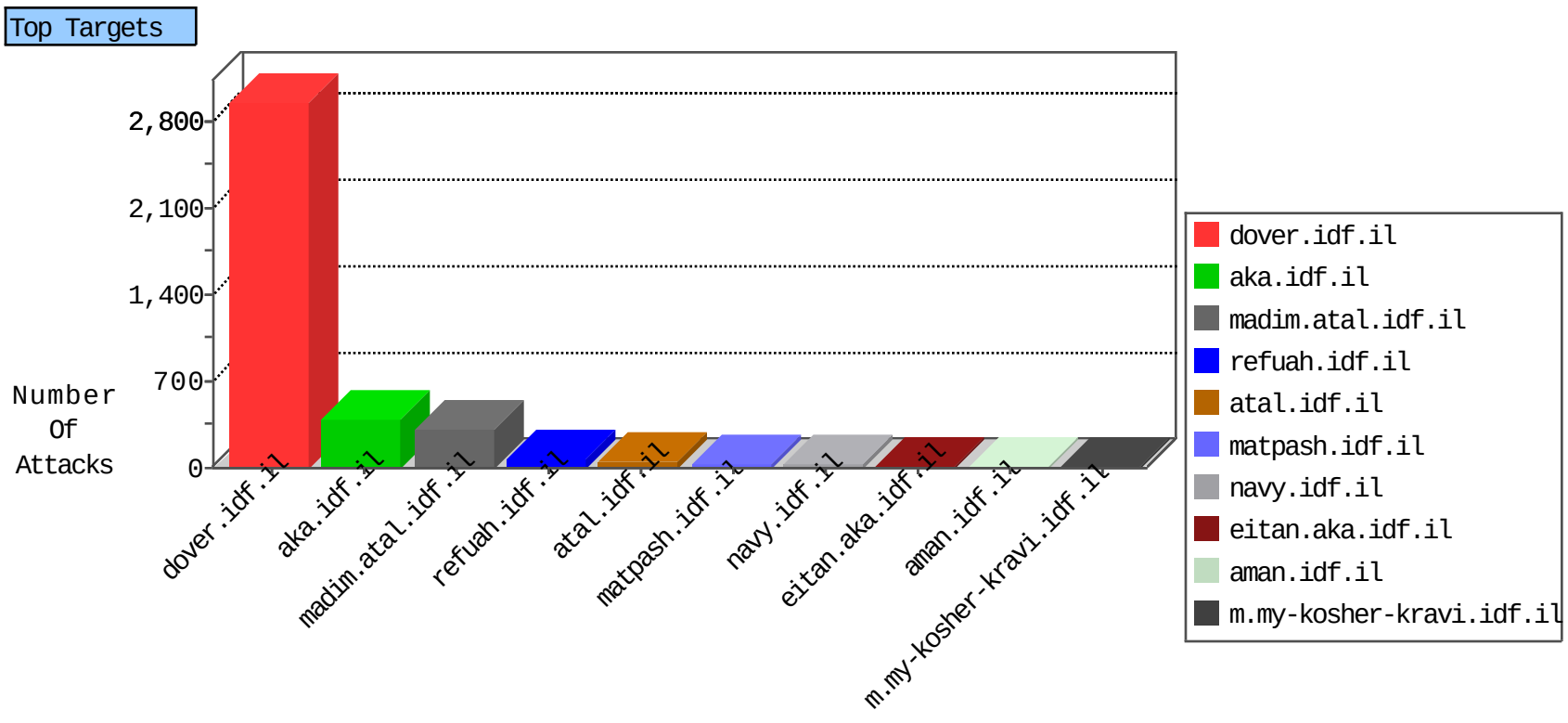
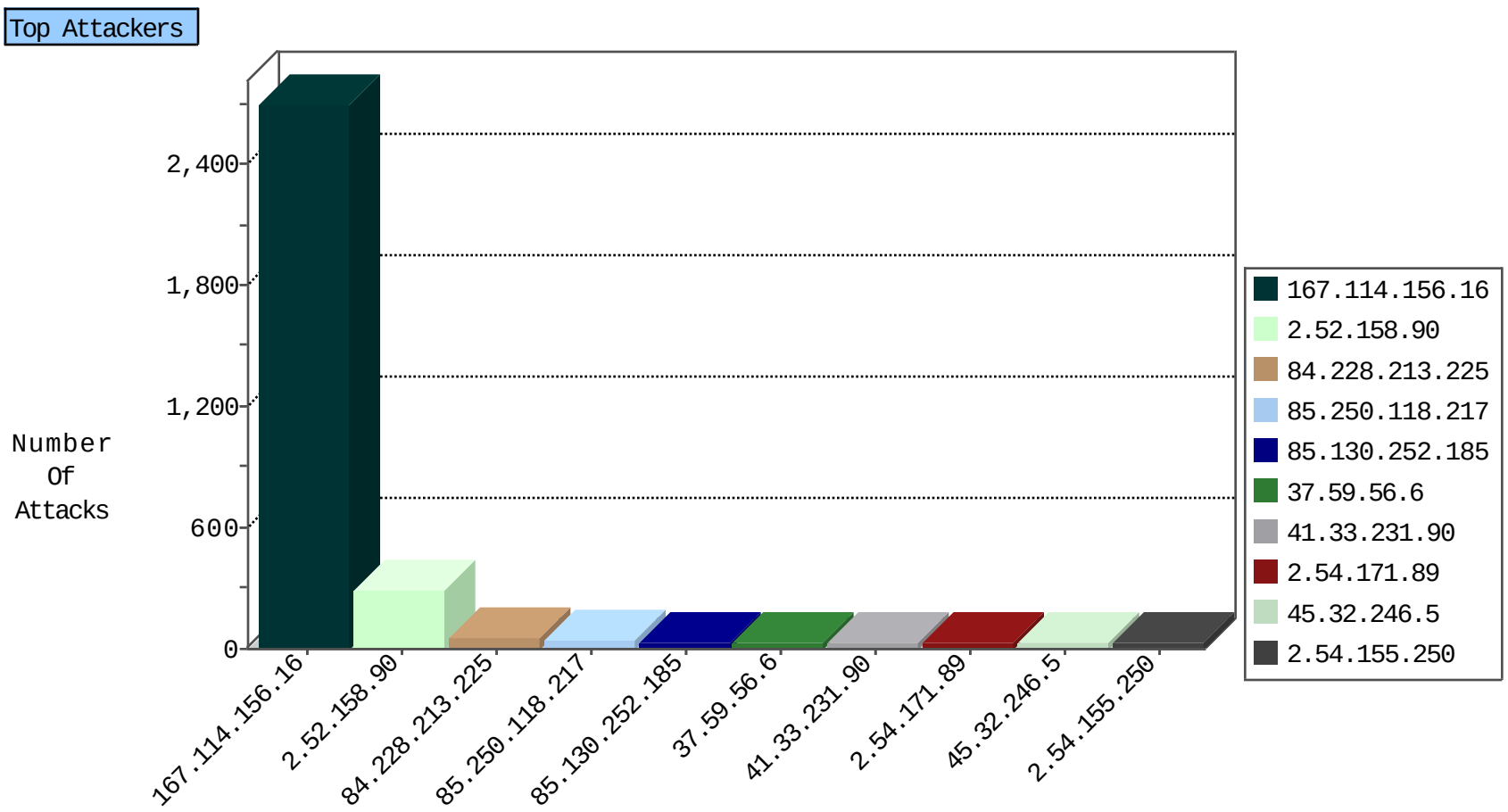
12-08-2015-19:04:00 to 12-08-2015-20:04:00

IDF Under Attack Daily Report



Top Target



Top Attackers

12-08-2015-19:04:00 to 12-08-2015-20:04:00

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	3320
45.32.246.5		147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	8
177.33.45.9	Brazil	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
177.33.45.9	Brazil	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
177.33.45.9	Brazil	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

12-08-2015-19:04:00 to 12-08-2015-20:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.59.56.6	France	147.237.77.216	dover.idf.i	19863: HTTP: WordPress Revslider/Showbiz PHP File Upload	Block	4
37.59.56.6	France	147.237.77.216	dover.idf.i	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.i	13840: TLS: OpenSSL Heartbeat Packet	Block	1

12-08-2015-19:04:00 to 12-08-2015-20:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.59.56.6	147.237.77.216	France	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.81.135	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
176.12.136.76	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	2
66.249.81.196	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
176.12.136.76	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	2
45.32.246.5	147.237.77.176		matpash.idf.il	ET SCAN Potential SSH Scan	1
43.229.53.89	147.237.0.19	Japan	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.196	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
119.73.228.130	147.237.77.227	Singapore	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
43.229.53.89	147.237.0.33	Japan	idf.il	ET SCAN Potential SSH Scan	1
43.229.53.89	147.237.0.16	Japan	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.196	147.237.76.177	China	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.26.149.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.67.1.109	147.237.77.121	United States	e.navy.idf.il	ET SCAN Potential SSH Scan	1
119.73.228.130	147.237.77.227	Singapore	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
119.73.228.130	147.237.77.227	Singapore	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1

12-08-2015-19:04:00 to 12-08-2015-20:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
84.228.213.225	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	46
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
109.66.139.227	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
85.250.118.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
85.250.118.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
79.180.35.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.116.236.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
109.64.229.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.252.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.85.137.110	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
45.32.246.5		147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
77.126.15.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
98.7.94.168	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
45.32.246.5		147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	7
85.130.252.185	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
85.130.252.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.130.252.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.171.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.79.35	United States	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.80.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.3.144.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.171.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
109.67.205.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.3.144.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.171.89	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.20.195	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.67.205.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.56.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.124.44	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.171.89	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
176.13.20.195	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.171.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.32.4	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.142.227.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.186.7.7	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.233	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.233	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.155.250	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
213.57.167.202	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
207.241.226.39	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	5
213.57.167.202	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.155.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.155.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
212.179.28.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.167.98	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

12-08-2015-19:04:00 to 12-08-2015-20:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.158.90	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.158.90	Block	145
2.52.158.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
2.52.158.90	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.52.158.90	Block	17
109.186.191.69	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.186.191.69	Block	17
31.210.186.147	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
176.13.13.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
37.59.56.6	France	147.237.77.216	dover.idf.il	PHP Attempt	Block	7
46.19.86.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.59.56.6	France	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 37.59.56.6	Block	6
37.59.56.6	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.59.56.6	Block	6
98.7.94.168	United States	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
85.250.152.97	Israel	147.237.0.34	tikshuv.idf.il	Parameter Type Violation searchText in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	4
80.230.93.129	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
176.13.17.187	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Byte Code Character in Parameter Name from 176.13.17.187	Block	3
93.173.39.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.17.187	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.17.187	None	3
176.13.22.104	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
89.138.231.139	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
79.179.127.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/undefined	Block	2
37.218.210.222	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	2
176.13.15.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
46.117.255.55	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
85.250.118.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
87.106.22.163	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/admin	Block	1
46.120.182.13	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 1	Block	1
46.19.86.126	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.148.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.213.225	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
37.59.56.6	France	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
109.66.139.227	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
79.178.21.252	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
217.132.22.158	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachaer	Block	1
46.120.182.13	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method [[#24]]Â´;s]Ã˜Ã¥FÂ–[[#14]]Â™3WdÃŠÃŠ*)Â“Ã–Â”Ã™Ã±Â©z^ÂŸ5Ã–RÃºÂˆÃ¹[[#11]]`aÂ¸Ã´Â”	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/6255.jpg	Block	1
2.52.158.90	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
46.120.182.13	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
176.13.17.187	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding Js/ in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
79.183.167.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.227.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.88.84.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.44.131.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
109.64.128.69	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.81.250	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
212.150.1.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
46.120.182.13	Israel	147.237.72.166	aka.idf.il	Malformed URL	Block	1
185.3.144.43	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.150.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.213.225	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1

12-08-2015-19:04:00 to 12-08-2015-20:04:00