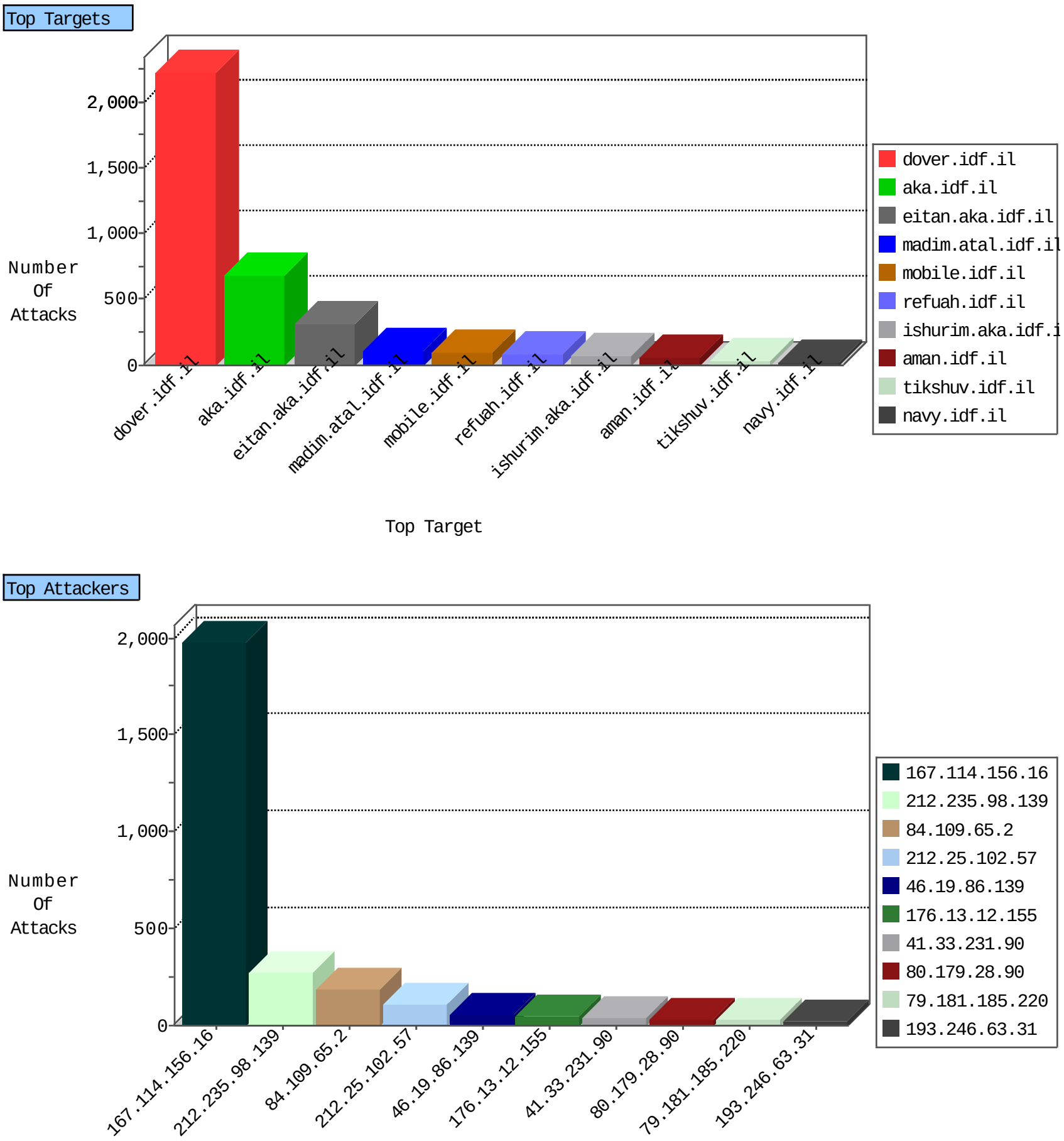
12-14-2015-15:04:08 to 12-14-2015-16:04:08

IDF Under Attack
Daily Report



12-14-2015-15:04:08 to 12-14-2015-16:04:08

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	DOS-Tool-SwitchbladG	dest-reset	3189
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
132.70.66.12	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
80.82.64.198	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
198.48.92.104	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
212.179.177.148	Israel	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1

12-14-2015-15:04:08 to 12-14-2015-16:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
193.246.63.31	Switzerland	147.237.77.216	dover.idf.il	16643: HTTP: Protected File Access (/proc/self/environ)	Block	2
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-14-2015-15:04:08 to 12-14-2015-16:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
193.246.63.31	147.237.77.216	Switzerland	dover.idf.il	Tehila - Perl LWP with fake user agent	4
212.179.177.148	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
109.65.115.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.205.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
216.250.117.56	147.237.77.176	United States	matpash.idf.il	Tehila - Perl LWP with fake user agent	1
198.20.69.74	147.237.76.39	United States	mobile.meitav.idf.i	ET DROP Dshield Block Listed Source	1
87.68.16.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.117.137.81	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
216.250.117.56	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
212.179.220.105	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.177.148	147.237.72.167	Israel	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

12-14-2015-15:04:08 to 12-14-2015-16:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	270
176.13.12.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
77.127.59.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.148.184	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
2.52.178.15	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.52.144.67	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.19.86.79	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
2.52.50.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.57.130.216	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
46.19.86.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.181.185.220	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
79.181.185.220	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
213.57.130.216	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.19.85.230	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
5.102.254.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
84.109.65.2	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.181.185.220	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
212.179.241.69	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.90.202.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.147	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.61.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.236.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.86.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.154.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.136	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.178.207.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.165.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.135.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
213.57.247.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.5	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.226.14.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.135.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.179.201.16	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.186.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
188.120.148.192	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.146.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.117.158.182	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
176.12.146.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.128.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
84.109.3.6	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
8.37.228.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
46.19.86.79	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence		monitor	4
176.12.139.114	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

12-14-2015-15:04:08 to 12-14-2015-16:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.109.65.2	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	180
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	104
46.19.86.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	56
80.179.28.90	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 80.179.28.90	Block	23
46.19.86.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
185.120.125.20		147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.120.125.20	Block	17
185.32.179.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
193.246.63.31	Switzerland	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	8
176.13.19.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
87.69.177.65	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	4
87.69.177.65	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	4
80.179.28.90	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/infocenteritem/browser.png"	Block	4
193.246.63.31	Switzerland	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 193.246.63.31	Block	4
193.246.63.31	Switzerland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/delete_all.php	Block	4
2.54.54.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.50.163	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
5.102.254.226	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/7/	Block	3
77.127.59.174	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.6.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.160.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
5.102.254.226	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.102.254.226	Block	3
46.116.183.142	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	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
2.54.167.93	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
216.250.117.56	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 216.250.117.56	Block	2
213.57.34.84	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
216.250.117.56	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
5.102.254.226	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/sip_storage/files/7/	Block	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
81.218.152.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hmas	Block	2
176.12.143.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
216.250.117.56	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
212.179.177.148	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 212.179.177.148 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	2
94.159.203.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.26.147.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.94.40.147	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
176.12.144.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.36.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
212.199.121.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.230.93.144	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/sip_storage/files/7/	Block	1
46.19.85.25	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method uvc=1%7C50; in URL __atuvs=566ebe6c76bd4186000	Block	1
197.134.130.4	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
85.64.72.43	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.102.254.226	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/sip_storage/files/7	Block	1
176.13.16.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.81.250	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
50.116.30.23	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
40.77.167.57	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1

12-14-2015-15:04:08 to 12-14-2015-16:04:08