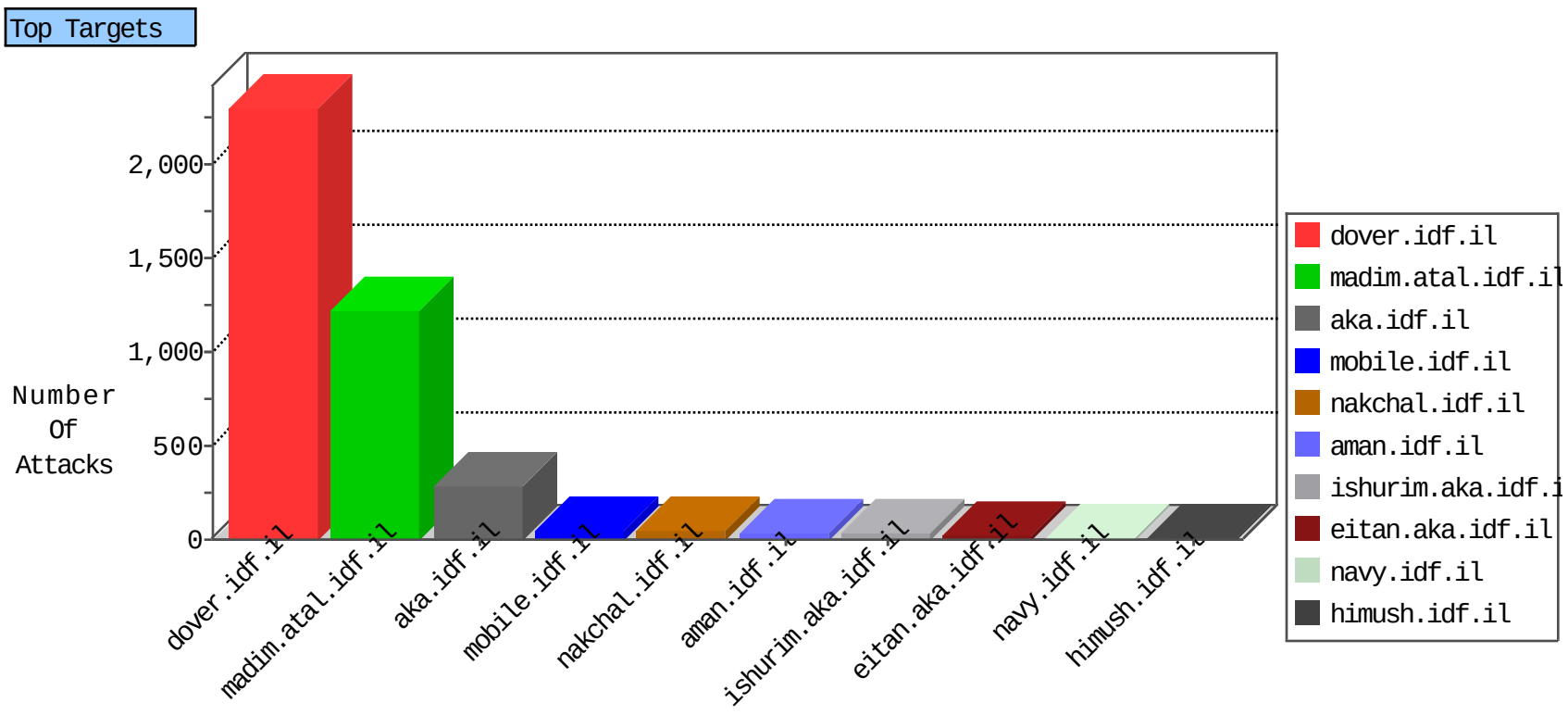
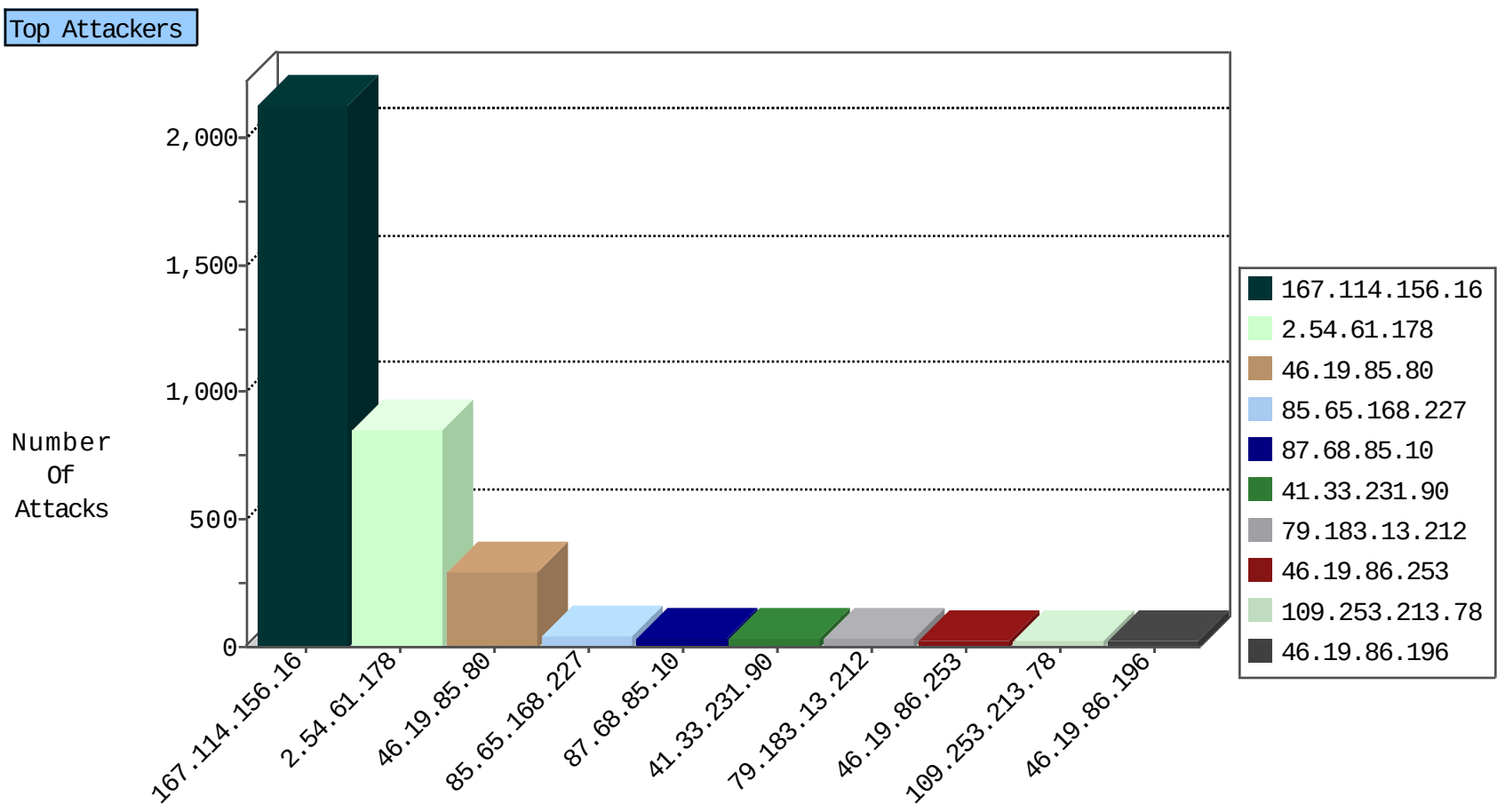
12-18-2015-14:04:00 to 12-18-2015-15:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-18-2015-14:04:00 to 12-18-2015-15:04:00

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	3108
109.65.102.254	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
188.138.33.34	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.66	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
188.138.33.34	Germany	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
185.106.94.126		147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.66	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
188.138.33.34	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.66	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

12-18-2015-14:04:00 to 12-18-2015-15:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
24.220.5.234	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
162.244.15.156	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

12-18-2015-14:04:00 to 12-18-2015-15:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
31.180.251.102	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN Potential SSH Scan	2
31.180.251.102	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN Potential SSH Scan	2
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.180.251.102	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
176.13.3.207	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
5.141.196.155	147.237.77.74	Russian Federation	law.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
5.141.196.155	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
5.141.196.155	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
211.215.19.235	147.237.72.166	Korea, Republic of	aka.idf.il	ET SCAN Potential SSH Scan	1
31.180.251.102	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN Potential SSH Scan	1
211.215.19.235	147.237.72.14	Korea, Republic of	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
31.180.251.102	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
189.76.1.156	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.180.251.102	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.141.196.155	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
5.141.196.155	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
5.141.196.155	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 2048	1
5.141.196.155	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -f -sS	1
211.215.19.235	147.237.72.156	Korea, Republic of	aman.idf.il	ET SCAN Potential SSH Scan	1
31.180.251.102	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
187.194.99.125	147.237.76.199	Mexico	e.nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.180.251.102	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1

12-18-2015-14:04:00 to 12-18-2015-15:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.183.13.212	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.86.196	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	19
109.253.213.78	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
87.68.85.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
87.68.85.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.86.16	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
85.64.120.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.224	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
85.65.168.227	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
213.57.128.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
37.46.39.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
85.65.219.188	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.86.77	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.179.202.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.172.140.71	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.102.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.38.90	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.22.129.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.106.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.211	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.165.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.209.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.146.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
62.0.104.162	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
77.125.7.48	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
41.66.172.8	South Africa	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
62.90.147.211	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
94.166.107.181	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.46.39.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
176.13.20.251	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.3.207	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
217.132.249.181	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
185.3.144.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.51.15	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.117.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.196	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.60.112	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.41.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.129.15	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.177.112.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-18-2015-14:04:00 to 12-18-2015-15:04:00

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
84.228.60.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-18-2015-14:04:00 to 12-18-2015-15:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.61.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	302
2.54.61.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	256
2.54.61.178	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.61.178	Block	209
46.19.85.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	133
46.19.85.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	129
2.54.61.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	84
85.65.168.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.85.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	27
46.19.86.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
46.19.85.80	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.80	Block	4
109.253.213.78	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.13.23.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.213.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
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
85.250.59.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	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
109.66.3.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.3.146.140	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
87.68.85.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
207.46.13.145	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
87.69.127.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.180	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.109.81.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.180.187.47	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.188.132	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.41.11	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
66.249.66.21	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1761	Block	1
213.8.204.12	Israel	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	1
80.246.136.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.136.104	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.126.14.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19550-he/dover.aspx	Block	1
93.172.33.52	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl60.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
84.111.12.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.180	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/9/size220x0/16949.jpg	Block	1
79.180.233.47	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	1
5.29.167.206	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/kkkkkkk=3b95da62kkkkkkk_3b95da62	Block	1
2.54.41.11	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 2.54.41.11	None	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.234.165	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.84	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to chimush.atal.idf.il/console/core/doc_mgr/null	Block	1
213.8.204.12	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1
207.46.13.131	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.131	Block	1
80.246.137.211	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.126.15.123	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

12-18-2015-14:04:00 to 12-18-2015-15:04:00