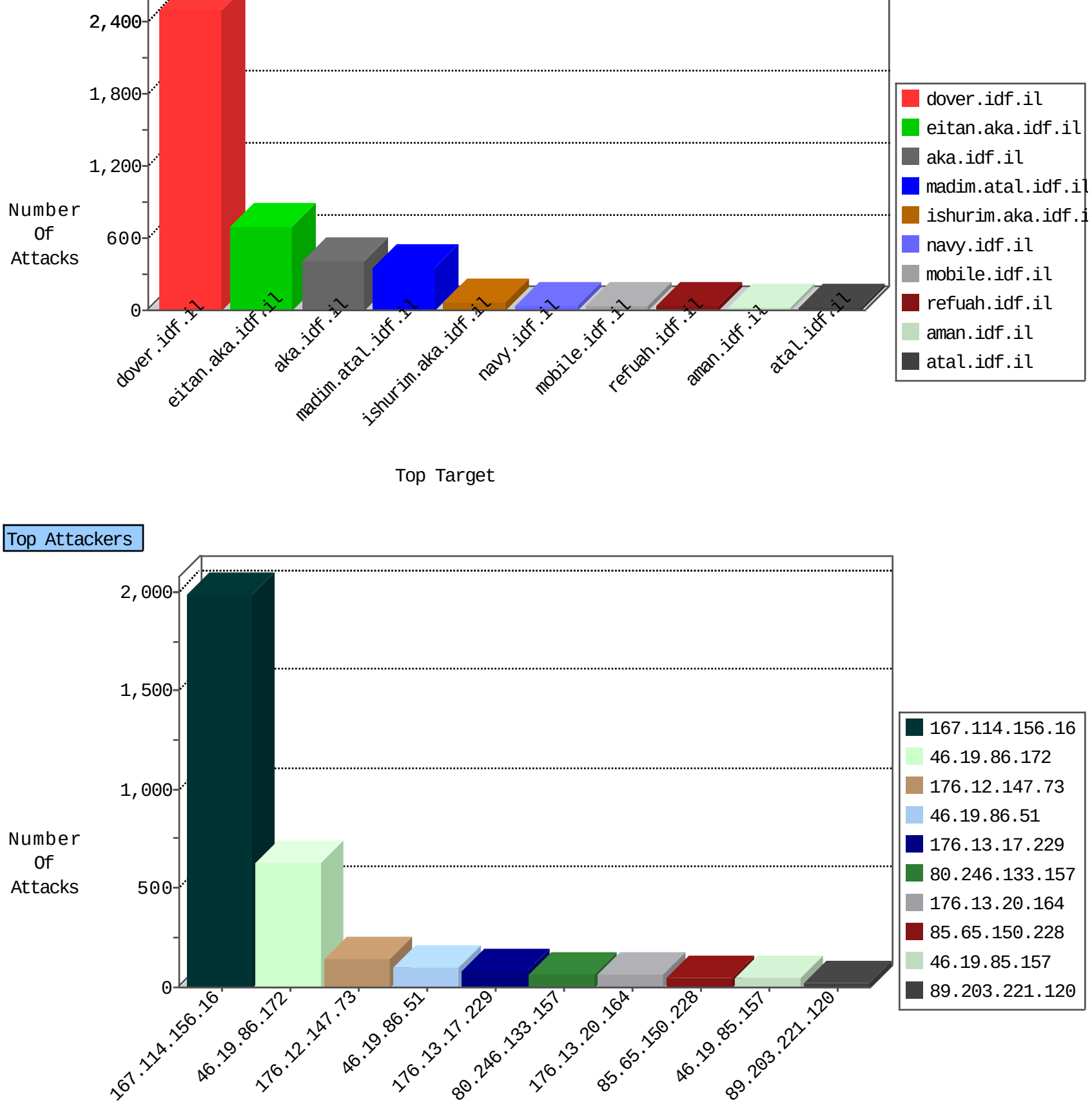
12-20-2015-15:04:05 to 12-20-2015-16:04:05

IDF Under Attack Daily Report



12-20-2015-15:04:05 to 12-20-2015-16:04:05

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	3095
176.13.20.164	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	39
146.185.57.7	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
176.13.12.193	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
46.19.85.135	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
134.147.203.115	Germany	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	2
46.19.86.161	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
61.182.170.38	China	147.237.76.177	ncore.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
61.182.170.38	China	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

12-20-2015-15:04:05 to 12-20-2015-16:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.203.221.120	Czech Republic	147.237.77.216	dover.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	18

12-20-2015-15:04:05 to 12-20-2015-16:04:05

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	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
179.252.20.234	147.237.76.42	Brazil	refuah.idf.il	ET SCAN Potential SSH Scan	2
134.191.232.68	147.237.77.170	Israel	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
179.252.20.234	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
139.196.36.18	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
121.201.61.50	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
93.172.137.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.10.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.22.43.252	147.237.72.166	Norway	aka.idf.il	ET SCAN Potential SSH Scan	1
79.183.36.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.114.91.229	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.147	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
179.252.20.234	147.237.76.147	Brazil	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
2.54.157.148	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.176.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
115.231.121.130	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
87.68.60.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.22.43.252	147.237.77.170	Norway	maarachot.idf.il	ET SCAN Potential SSH Scan	1
84.109.240.171	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.199.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
179.252.20.234	147.237.76.200	Brazil	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
43.245.183.201	147.237.76.38	Japan	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
179.252.20.234	147.237.76.86	Brazil	navy.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1

12-20-2015-15:04:05 to 12-20-2015-16:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.86.172	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	537
85.65.150.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
46.19.85.157	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	45
2.52.173.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.121.59.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.54.184.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
79.177.101.13	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
80.246.133.157	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.20.164	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
176.13.20.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
46.19.86.50	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.172	Israel	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
176.13.21.92	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.78.147	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.89	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.2.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.89	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.215.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.181.27.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.123	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.48	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.172	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.181.224.199	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.177.215.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
62.219.198.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.172	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.34	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.228.218.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.34	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.228	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.21.92	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
62.219.198.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5

12-20-2015-15:04:05 to 12-20-2015-16:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	98
176.13.17.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
176.12.147.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
46.19.86.172	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	75
176.12.147.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	69
80.246.133.157	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
81.218.125.103	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.125.103	Block	18
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 192.115.64.250	Block	7
211.123.214.30	Japan	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 211.123.214.30	Block	5
46.19.86.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
62.90.179.245	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	3
5.29.13.216	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
176.12.145.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.5.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.65.60.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
91.143.80.201	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
80.246.139.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.46.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.117.56.120	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
59.120.160.173	Taiwan	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
46.117.108.85	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	2
79.176.118.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
213.151.49.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.199.57.201	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	2
176.13.12.94	Israel	147.237.0.19	madim.atal.idf.i	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
2.54.32.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
195.189.193.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
79.177.215.84	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.51	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.51	Block	1
150.70.188.175	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
37.26.147.145	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
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	1
73.129.219.228	United States	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 73.129.219.228 (Unknown SSL Session)	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
2.54.43.180	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/text.css	Block	1
81.218.125.103	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/[object object]	Block	1
46.116.143.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.179.119.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.127.125.71	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
198.58.102.96	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
5.28.179.53	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.12.57	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
46.121.156.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.17.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.142.143	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl25 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.86.106	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/tfasim.aspx.	Block	1

12-20-2015-15:04:05 to 12-20-2015-16:04:05