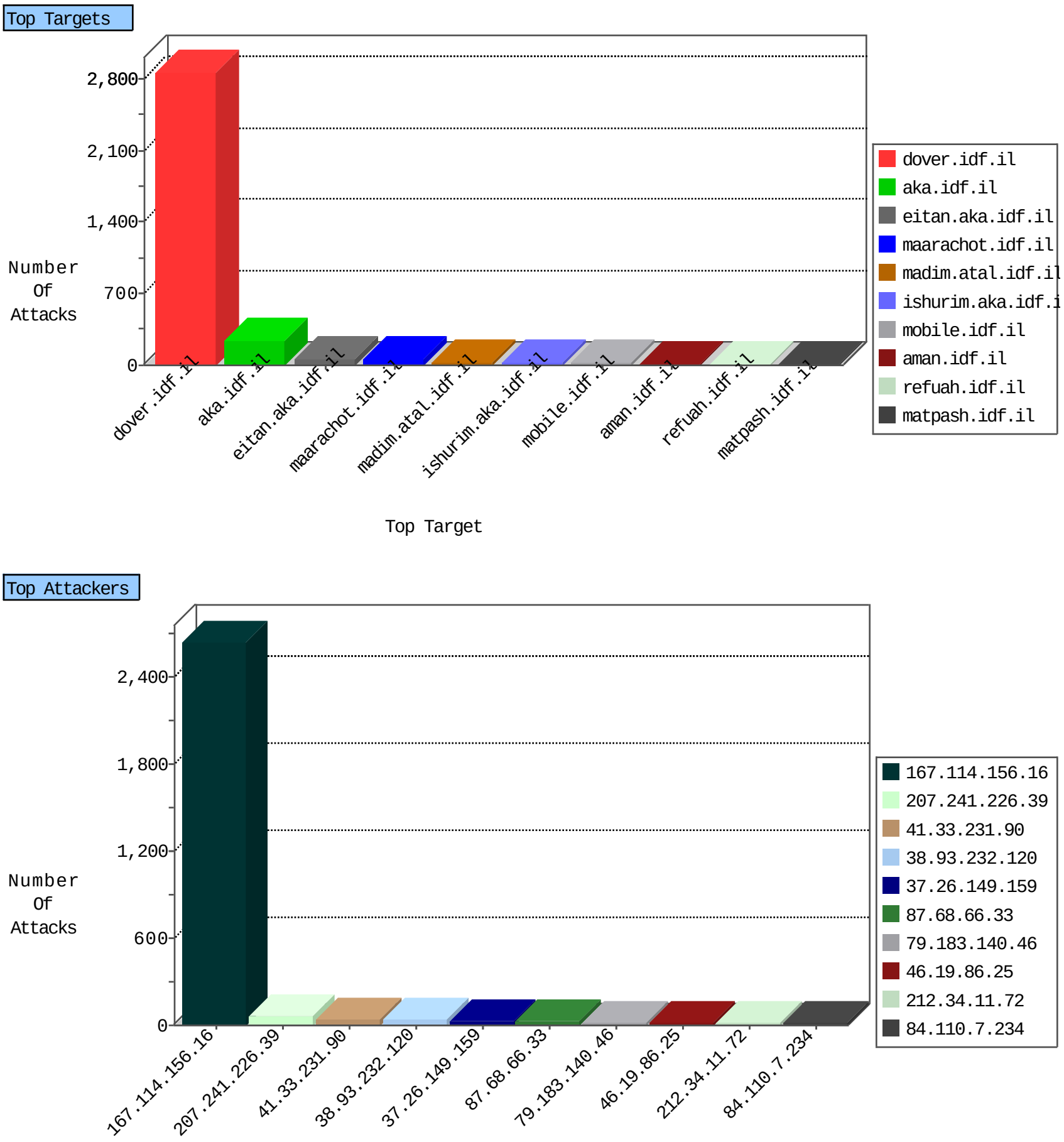
12-10-2015-21:04:00 to 12-10-2015-22:04:00

IDF Under Attack Daily Report



12-10-2015-21:04:00 to 12-10-2015-22:04:00

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	3366
84.110.7.234	Israel	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	6
84.110.7.234	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
115.231.222.40	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2

12-10-2015-21:04:00 to 12-10-2015-22:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.252.131.34	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-10-2015-21:04:00 to 12-10-2015-22:04:00

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
66.249.79.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.74.105	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
61.182.170.38	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
46.151.55.35	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
40.115.58.160	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
201.172.77.216	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.106.129.219	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 2048	1
78.193.2.8	147.237.0.19	France	madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
61.182.170.38	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
40.115.58.160	147.237.76.38	United States	e.e.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
201.172.77.216	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.106.129.219	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 3072	1
113.59.33.61	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -f -sS	1

12-10-2015-21:04:00 to 12-10-2015-22:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.26.149.159	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
87.68.66.33	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
38.93.232.120	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
38.93.232.120	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
79.183.140.46	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
213.57.13.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
5.22.134.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.64.51.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
207.241.226.39	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.181.4.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.68.18.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.86.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.175.180	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.165.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.32.179.196	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.117.73.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.182.170.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
80.246.136.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.183.140.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.151.35.218	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.65.27.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.50.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.64.120.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.108.172.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.75.30	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.65.175.180	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.12.148.164	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.181.4.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.176.114.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
82.81.5.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.64.51.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
185.32.179.49	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
84.110.7.234	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.178.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.170.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.34.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.241.226.39	United States	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.110.144.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.145.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.204.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.115.132.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.172.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-10-2015-21:04:00 to 12-10-2015-22:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.241.226.39	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 207.241.226.39	Block	46
207.241.226.39	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.241.226.39	Block	8
87.68.18.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
212.34.11.72	Jordan	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	6
212.34.11.72	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 212.34.11.72	Block	5
212.34.11.72	Jordan	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	5
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	4
85.65.102.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
93.172.11.239	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.172.11.239	Block	3
37.26.148.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
159.203.70.162	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 159.203.70.162	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
87.68.243.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.169.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.182.116.244	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
84.109.106.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18719-he/dover.aspx	Block	1
46.117.73.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.116.244	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version Ãµu<gtsEÂ¶ÃŠp[[#25]]Â?Â¬Â?Â˜Âž >jcqÂ¹B[[#31]]Â²Â?ÂŸÂ›3ÃžÃ›\ Â‡Â•[[#29]]Â¥Ã†ÃŽÂ¦Ã?~eÃ–[[#0]]/ Ã¶G[[#28]]Â›Ã£sÂ’Â³Ã„Â½Â£Ã¥Â‰Ã›e[[#30]]Ã’Ã?Â¥1!Â” [[#22]][[#2]]F[[#2]]hÂªÂ‹VÃ‹WÃ?gfÂ±.[[#14]][[#25]]<pÂŒg@Ã–m ~Ã‰Â±)Â—UoaÂ°Un/KÃ‚Ã¯Ã¾ÂœÃ• Â°2[[#21]]Â¯Ã¸XYÃ?!Ã¡Ã®Ã¦;Ã²Â?Â-Âƒ{[[#30]]Ã…*Ã–4Â• Â?Â°xg[[#31]][[#12]]Â²Â¤[Ãª[[#8]]Ã-FÂ°Ã hhkÃ¹ Ã…Å¡ [[#26]]Ã-(Ã?Ã¶@b[[#1]][[#31]]Ã°ÂœÂª!Ã±Â£ÃµCÃœDÃŸ5Ã²Ã§[[#8]]Â‡ ~CÃ©Ãƒ$NÂ«(Ã´[Ã„5]7GX$KÂ§5/Ã‚ERÃ‚Â´Ã [[#15]]Ã„ >Â Ã³Ã¼Â¸Ã»Ã ng~ Ã¹Â?Â–^5&Â²zÂ‰Â…Â°Ã•[[#30]]0Â¤VÃ’Â?K[[	Block	1
37.142.68.51	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.181.4.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1
52.53.228.65	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/miluim/templates/inner.asp	Block	1
185.27.105.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
81.220.95.14	France	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
79.182.116.244	Israel	147.237.72.166	aka.idf.il	Distributed Malformed HTTP Header Line	Block	1
41.45.195.55	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
109.66.27.224	Israel	147.237.72.166	aka.idf.il	Unknown Parameter y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
89.139.166.191	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.230.57	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
5.102.233.92	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
85.64.247.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	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
46.120.156.17	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.156.17	Block	1
159.203.70.162	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
79.182.116.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
37.142.68.51	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
79.182.116.244	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
212.34.11.72	Jordan	147.237.77.216	dover.idf.il	Malformed URL http/1.1	Block	1
2.54.5.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
81.220.95.14	France	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
54.153.32.246	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
79.182.116.244	Israel	147.237.72.166	aka.idf.il	Distributed NULL Character in Header Name	Block	1
46.19.85.123	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.aspx.	Block	1
109.160.146.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
8.37.70.36	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1177-he/refuah.aspx&usg=alkjrhjepyaivcozsjkoc9pp7ylpuj9rla	Block	1

12-10-2015-21:04:00 to 12-10-2015-22:04:00