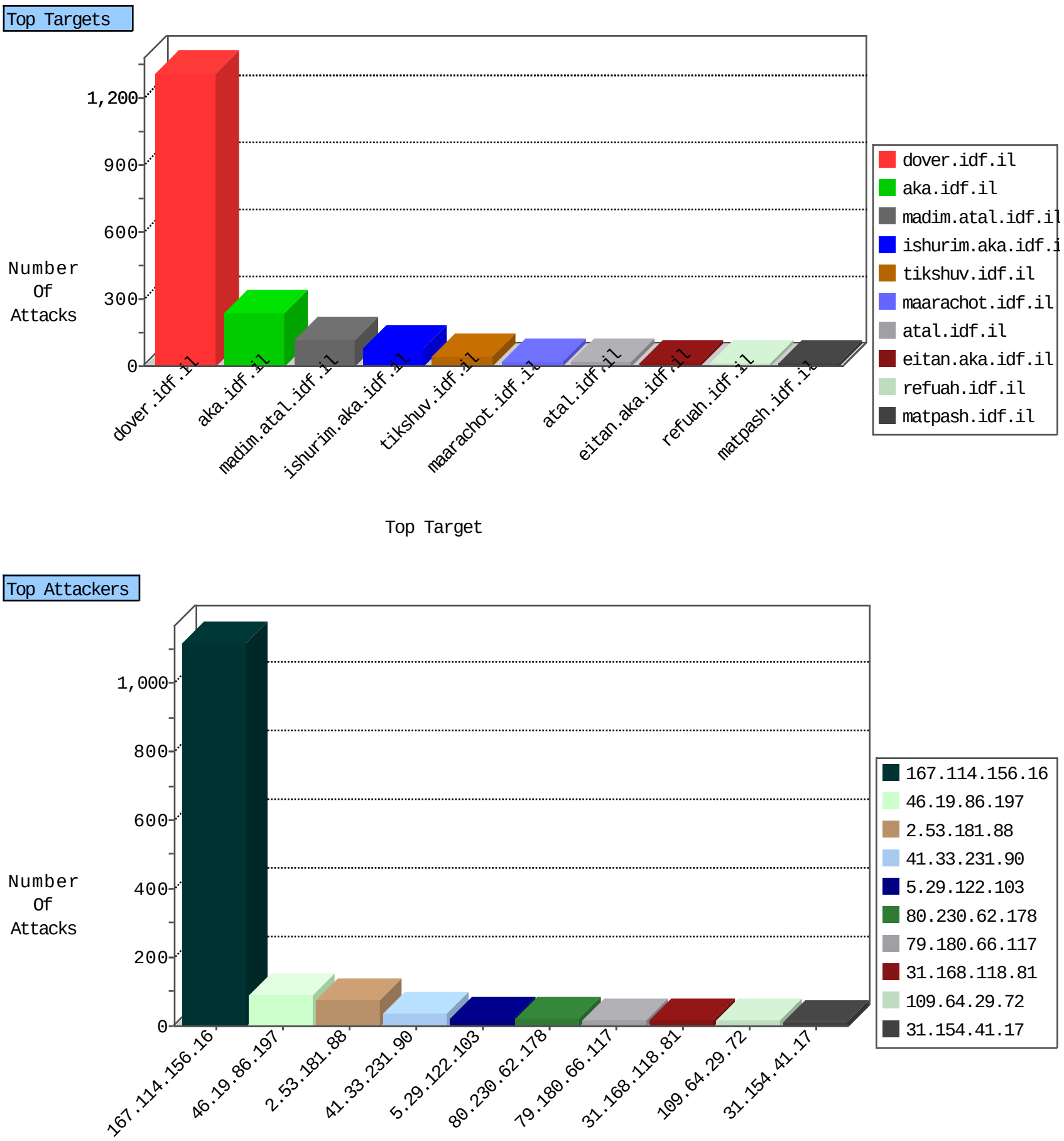
04-14-2016-17:04:07 to 04-14-2016-18:04:07

IDF Under Attack
Daily Report



04-14-2016-17:04:07 to 04-14-2016-18:04:07

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	Block_Ip_Web_In	drop	1120
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
82.145.219.191	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	1

04-14-2016-17:04:07 to 04-14-2016-18:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.122.103	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	19
213.8.204.71	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
207.241.237.222	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
213.8.204.61	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
69.30.221.250	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
176.13.3.223	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.158	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
150.70.173.43	Japan	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-14-2016-17:04:07 to 04-14-2016-18:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
31.154.41.17	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	11
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
84.144.247.241	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
80.230.62.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.111	147.237.77.216	Europe	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.21.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.147.229	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.140.178.61	147.237.77.216	Oman	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.200.119	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.172.236.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.60.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.209.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.221.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
191.187.83.144	147.237.0.34	Brazil	tikshuv.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.138.16.119	147.237.77.216	Brazil	dover.idf.il	portscan: TCP Distributed Portscan	1
95.106.100.67	147.237.77.216	Russian Federation	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.161.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

04-14-2016-17:04:07 to 04-14-2016-18:04:07

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
2.53.181.88	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	23
2.53.181.88	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
80.230.62.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
2.53.181.88	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
109.64.29.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.53.181.88	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.181.153.89	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
31.44.141.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
41.46.184.154	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
80.246.139.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
62.219.209.208	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.180.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.173.154.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.227.184	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.243.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.118.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
80.246.136.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
96.52.151.38	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
96.52.151.38	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
31.168.118.81	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
109.253.197.38	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.3.144.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.55.62.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.159.180.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.246.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.28.164.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.235.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.4.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
132.66.76.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.22.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.198.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.242.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.98.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.199.34.114	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	3
62.219.136.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.121.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.20.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.169.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.123.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.23.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
70.199.64.212	United States	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.181.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-14-2016-17:04:07 to 04-14-2016-18:04:07

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
185.3.144.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.30.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.154.171.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.234.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
176.13.5.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
2.53.19.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
37.26.146.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.143.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.44.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.66.117	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.53.61.42	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
185.27.105.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.138.226.241	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 89.138.226.241	Block	2
79.183.189.84	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	2
2.53.61.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
87.71.34.133	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/tfasim.aspx'	Block	2
79.183.189.84	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	2
89.138.226.241	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.249.66.5	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/moreinfo/tichnun.yosh@gmail.com	Block	1
31.154.41.17	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
79.180.66.117	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method q´,?e®#ìNcÏš½Ñ;í[[#2]]_q¨A“žn[[#22]]Dª+?Bþõ[[#28]]¸[[#31]]ÇÕï$Ô•—Z[[#1]]M[[#4]]NXMI[[#30]]Q[[#0]]—#012‘ in URL [[ף*›ך#11]]11#[[s¯]]Ɒz9ת/›˛Û˛x‡€l[[#6]]ע֗ר[[#14]]¸-lm[[ם#20[[Ÿ]]#5„mea¼û¶210#µ+)•¬]]®4•qc&¶_ɒpljf[[#30]]÷[[#19]]5[[#26]][[#2]]’	Block	1
79.180.66.117	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 3	Block	1
74.208.16.40	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18503-en/dover.aspx	Block	1
138.134.102.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
84.94.77.101	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.120.128.235	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.66.117	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 79.180.66.117	Block	1
5.39.222.159	Netherlands	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
176.13.14.166	Israel	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-he/cogat.aspx	Block	1
79.180.66.117	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name ÕÉB˜©>µu²Ý”7!u’¼	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
79.180.66.117	Israel	147.237.72.166	aka.idf.il	Malformed URL [[ף*›ך#11]]11#[[s¯]]Ɒ9zת]]6#[[l€‡x˛Û˛›/ךŽעml-˛]]41#[[rם[[#20]]Ÿ[[#5]]¬•)+µ#012¶û¼aem„®4•qc&¶_ɒpljf[[#30]]÷[[#19]]5[[#26]][[#2]]’	Block	1
212.199.154.194	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/bottomcap.gif	Block	1
79.178.169.172	Israel	147.237.76.39	mobile.meitav.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	1
157.55.39.217	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18063-he/dover.aspx	Block	1
79.180.66.117	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at Ã¶X]nP×Œ±Ó[[#6]][[#5]]ž[[#7]]‹àšRV[[#27]]ûÎ[[#16]]G •Ë[[#19]]l[[#17]]•[[#27]]<![[#11]]ôðèÂ[[#3]]«Œ©›#012öôì[[#27]]ROã'.j[[#30]](ÿÆtC[[[#19]]n,ó#012!â¯[[#15]]´ƒœî•{cZ¼X~ìQï[[#20]]¯Ôµ[[#27]][[#0]][[#24]]d¾ê[[#23]]¬[[#24]]Åüñüø¾¨f[[#29]]M÷[[#21]]b}[[#28]]J%{™•[=~„[[#2]]ÆÜÙY[[#28]]öBgU»NÒÕ‰†úKD6a•ò¾<ô•[[#23]]Õö}*ðÙSSÉÄ×`Z•q¡2[[#11]]'[[#31]]ƒ•ãŽ[[#18]]ƒÚµYnüÔð©±ƒ<y@°ÐíŒÀA[[#23]][[#20]]MÃÙ/’ÁçÀz-n	Block	1
5.255.253.75	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
176.77.80.242	Russian Federation	147.237.0.15	kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.15/	Block	1
79.180.66.117	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
95.234.233.159	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.66.117	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.180.66.117	Block	1
213.254.241.4	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Abnormally Long Request method	Block	1
79.180.66.117	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
87.71.124.134	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
8.37.70.36	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1507-en/dover.aspx&usg=alkjrhh9althmfvq6egytellfqz5wrnjag	Block	1
79.180.66.117	Israel	147.237.72.166	aka.idf.il	NULL Character in Method q´,?e®#ìNcÏš½Ñ;í[[#2]]_q¨A“žn[[#22]]Dª+?Bþõ[[#28]]¸[[#31]]ÇÕï$Ô•—Z[[#1]]M[[#4]]NXMI[[#30]]Q[[#0]]—#012‘	Block	1
180.73.0.29	Malaysia	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
79.180.66.117	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method q´,?e®#ìNcÏš½Ñ;í[[#2]]_q¨A“žn[[#22]]Dª+?Bþõ[[#28]]¸[[#31]]ÇÕï$Ô•—Z[[#1]]M[[#4]]NXMI[[#30]]Q[[#0]]—#012‘	Block	1