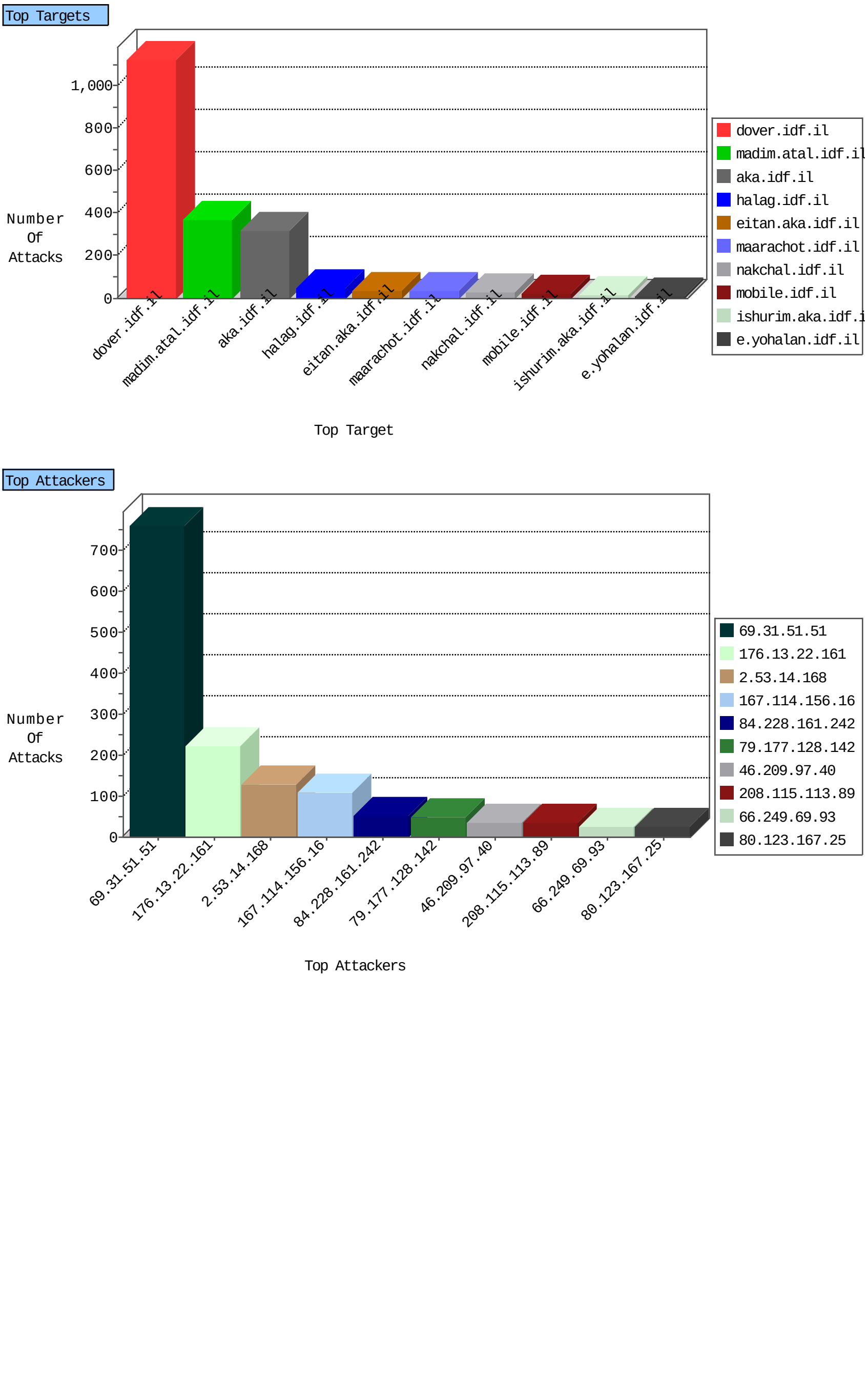
04-20-2016-15:04:06 to 04-20-2016-16:04:06

IDF Under Attack Daily Report



04-20-2016-15:04:06 to 04-20-2016-16:04:06

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	TCP handshake violation, first packet not syn	drop	15755
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	7157
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1163
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	18
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	9
37.26.147.221	Israel	147.237.76.31	nakchal.idf.il	Invalid TCP Flags	drop	5
198.20.69.74	United States	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1
222.186.50.253	China	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Http	drop	1

04-20-2016-15:04:06 to 04-20-2016-16:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.246.49.97	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.246.49.97	France	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4

04-20-2016-15:04:06 to 04-20-2016-16:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.246.49.97	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	15
31.168.3.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.158.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.173.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
103.29.216.158	147.237.72.166	Australia	aka.idf.il	SERVER-WEBAPP admin.php access	1
91.218.246.103	147.237.77.19	Russian Federation	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
91.218.246.103	147.237.76.148	Russian Federation	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.106.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.111.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.41.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.70	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
93.174.95.124	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
91.218.246.103	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
88.254.109.108	147.237.77.216	Turkey	dover.idf.il	portscan: TCP Distributed Portscan	1
80.74.103.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.172.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
219.83.163.168	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.45.137.76	147.237.76.31	Turkey	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
212.199.66.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-20-2016-15:04:06 to 04-20-2016-16:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
69.31.51.51	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	762
84.228.161.242	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
46.209.97.40	Iran, Islamic Republic of	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
80.123.167.25	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
37.26.146.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
79.180.52.201	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
207.241.229.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
79.177.128.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
2.53.182.37	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
212.150.127.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.93.15	Europe	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	12
46.19.86.110	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
87.70.19.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.80.126.166	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
216.4.56.153	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.209.97.40	Iran, Islamic Republic of	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.177.239.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.221	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.180.142.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.7.227	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.37.164	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.139.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.30.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
213.125.23.90	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.178.134.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
185.3.144.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.80.126.198	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
59.39.53.242	China	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
79.177.172.105	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.46.39.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.116.228.224	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.4.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.241.255	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.91.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.15.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.69.126	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.139.254	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.183.153.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-20-2016-15:04:06 to 04-20-2016-16:04:06

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

04-20-2016-15:04:06 to 04-20-2016-16:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.22.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	218
2.53.14.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	128
2.55.155.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
213.151.49.138	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	4
46.19.86.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
103.29.216.158	Australia	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 103.29.216.158	Block	3
46.19.86.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
103.29.216.158	Australia	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
109.253.226.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.177.128.142	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
85.130.244.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.177.128.142	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.177.128.142	Block	2
79.177.128.142	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 79.177.128.142	Block	2
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
217.156.163.66	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	2
79.177.128.142	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 79.177.128.142	Block	2
79.177.128.142	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 79.177.128.142	Block	1
123.125.71.40	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	1
103.29.216.158	Australia	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
79.177.128.142	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
46.19.86.53	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/text.css	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
79.177.128.142	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method ž:j”>ÖÆå‹Æª in URL `[[ɒı#8ɔ′¸]] c¬[[#20]]÷%[[#5]][[<ƾ#1·l]]02#[[v]]ɤDp[[22#]]ɾ`'[[32#]],ojˉɒž÷xg²‹>/¨Œ—[[#24]]wÛm·€fÿÚ¸ü•[[#22]]¯ɾ#·[´Ž:f6•-[[#1]]4yɲ¿g°	Block	1
79.177.128.142	Israel	147.237.72.166	aka.idf.il	Multiple Illegal URL Path Encoding from 79.177.128.142	Block	1
79.177.128.142	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version öÉHqÝæ[[#27]]:9Š¼âY£»zN€f&7wµ»[[#24]][[#6]][[#4]]pZ05Ü¸[[#23]]•xç[[#17]]¸¯õ[[#29]]•}Fád/×†x¦fÝ[[#25]][[#0]]lò[[#15]][[#1]]M›£E0>Ö’B¾I4÷±[[#16]]À{êñÿÍ•}yŽQUÐ¡°C[[#28]]”bKœ[[#18]]w®¥¹ šU÷ž3\ò0nÓÕPn^	Block	1
109.64.149.77	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
66.249.69.126	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in www.aka.idf.il/lomdim/forum/asp/showforum.asp	None	1
219.74.180.14	Singapore	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.128.142	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at [[#31]]ñGéeM®\[[#24]]\G*¡°A¿–[[#16]]“”[[#23]]šÁo^¨[[#4]]ü[[#0]][[#2]]Œ¢í‰[[#16]]+-^[[#20]]ñHþHõ[[#6]]ùâuÜ#Ÿ½Mç¯ü€ÐQä†U[[#21]]]F•[[#25]]ÂnÖìõfâh	Block	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.7.227	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
103.29.216.158	Australia	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 103.29.216.158	Block	1
79.177.128.142	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	1
79.177.239.172	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
197.40.0.184	Egypt	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
79.177.128.142	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 79.177.128.142	Block	1
79.177.128.142	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding `[[ɒı#8ɔ′¸]]c¬[[#20]]÷%[[#5]][[<ƾ#1·l]]02#[[v]]ɤDp¯ɾ#·[´Ž:]]xg²‹>/¨Œ—[[#24]]wÛm·€fÿÚ¸ü•[[#22÷žˉɒoj,]]#23[[']ɾ]]#22[[f6•-[[#1]]4yɲ¿g°;Ÿ~«[[#2]]ÿ˜¬	Block	1
109.65.30.171	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
87.70.67.111	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
79.177.128.142	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
220.255.146.215	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.177.128.142	Israel	147.237.72.166	aka.idf.il	NULL Character in Parameter Name [[ɣ#30[[′-]]#27X]]ƿ•ƒXdr‹·ɔ~y*;W:[[0#]]ÿ{¸Ù′₪:o™{¾¡b~zd•n×o{xS¥[[\ɿ7#27Jy—]]32#[[‡S]]ɤ7û¯Y‰hXK#·¯¯/&?Lב›OƆXשלɲ}{1%±+½}]]#31[[ɣ—&h{¡kvλpˈe]]#8[[%=•7₪ɣ]]l4[[#28₪*½0„Ÿ″2"פ:in €iÞn :¹′:š	Block	1
203.127.96.228	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.177.128.142	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 79.177.128.142	Block	1
79.177.128.142	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method ž:j”>ÖÆå‹Æª	Block	1
59.39.53.242	China	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/../shared/usercontrols/headerupper/	Block	1
79.177.239.172	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	1
197.40.0.184	Egypt	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1

04-20-2016-15:04:06 to 04-20-2016-16:04:06