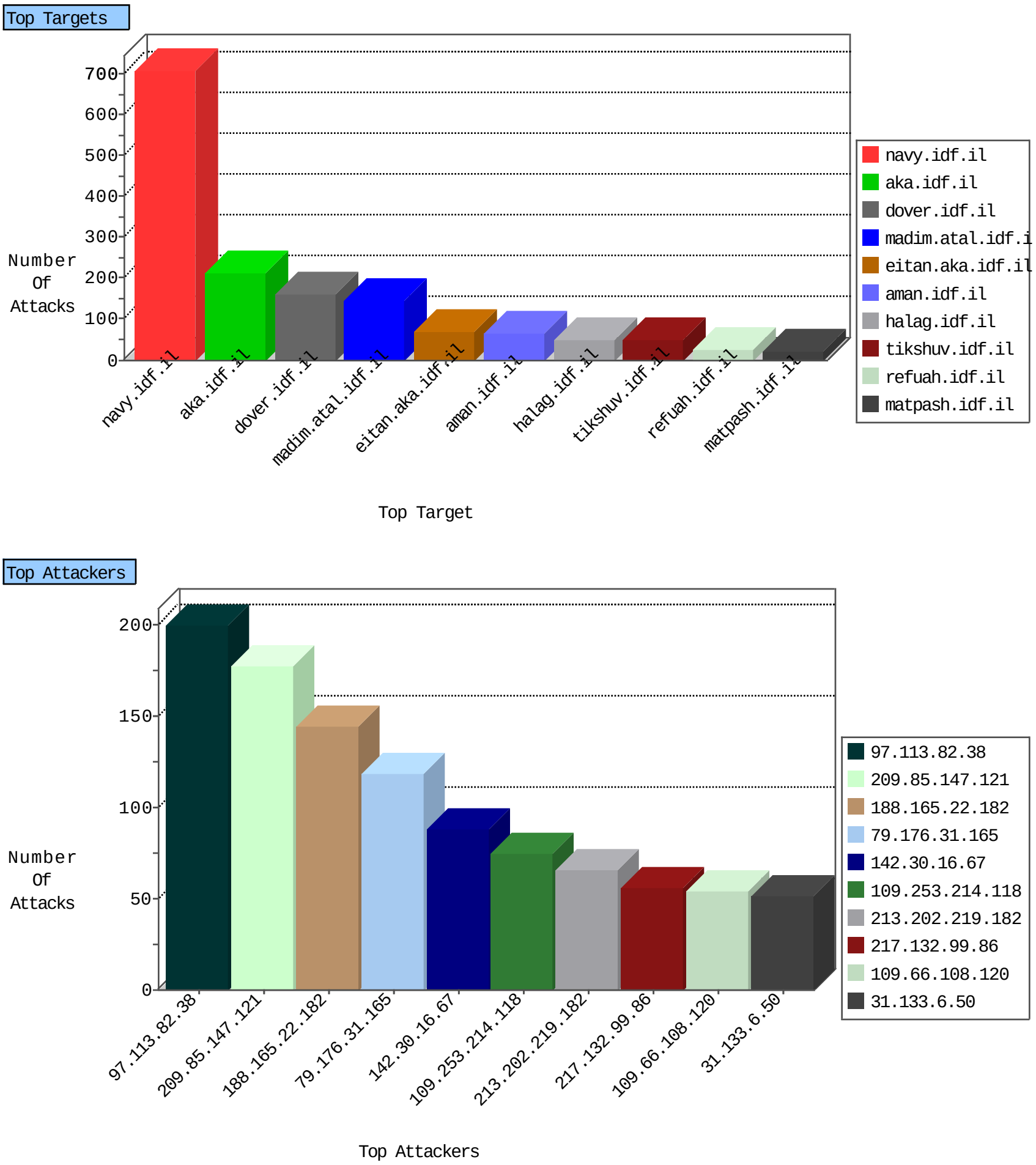
09-07-2016-22:04:07 to 09-07-2016-23:04:07

IDF Under Attack
Daily Report



09-07-2016-22:04:07 to 09-07-2016-23:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.155.67	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
46.19.85.137	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
2.53.149.4	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
51.254.172.96	France	147.237.76.176	test.ncore.idf.il	Black List	drop	1
71.6.216.44	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
51.254.172.96	France	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

09-07-2016-22:04:07 to 09-07-2016-23:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.102.49.190	Netherlands	147.237.77.179	e.mazi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-07-2016-22:04:07 to 09-07-2016-23:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
93.173.67.197	147.237.72.167	Israel	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
45.79.71.122	147.237.0.34	United States	tikshuv.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
61.240.144.65	147.237.0.200	China	m4u.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
200.58.214.138	147.237.72.156	Colombia	aman.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.208.193	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.204.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
200.58.214.138	147.237.72.156	Colombia	aman.idf.il	ET SCAN NMAP -sS window 3072	1
198.20.69.98	147.237.76.34	United States	yohalan.idf.il	ET DROP Dshield Block Listed Source	1
163.172.169.150	147.237.76.39	United Kingdom	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1

09-07-2016-22:04:07 to 09-07-2016-23:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
97.113.82.38	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	199
209.85.147.121	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	150
188.165.22.182	Poland	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	142
79.176.31.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	101
142.30.16.67	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	80
217.132.99.86	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	56
31.133.6.50	Poland	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	42
209.85.147.121	United States	147.237.76.86	navy.idf.il	SYN Attack		monitor	14
87.68.13.247	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
88.101.183.181	Czech Republic	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
88.101.183.181	Czech Republic	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.137	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
46.19.85.137	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
37.76.212.65	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	11
80.246.130.231	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
185.120.124.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
77.124.13.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.55.160.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
31.133.6.50	Poland	147.237.76.86	navy.idf.il	SYN Attack		monitor	9
2.55.155.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	9
176.13.236.52	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
109.253.245.119	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.86.245	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
87.68.28.20	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
2.53.177.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.66.211	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
109.64.73.36	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
109.253.245.119	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	6
109.253.138.119	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.155.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.55.155.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.94.72.92	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
200.114.215.51	Argentina	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	5
2.55.155.67	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
2.55.155.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.55.155.67	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
109.253.245.119	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		alert	4
109.186.75.173	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
84.110.234.111	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
94.230.86.189	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
131.253.27.194	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
209.85.147.121	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
200.114.215.51	Argentina	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.53.144.165	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
209.85.147.121	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	4
213.202.219.182	Germany	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
213.202.219.182	Germany	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.13.236.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
200.114.215.51	Argentina	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
213.202.219.182	Germany	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

09-07-2016-22:04:07 to 09-07-2016-23:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.214.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	75
109.66.108.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
81.218.101.66	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	6
213.57.59.50	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	6
81.218.101.66	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	5
77.138.138.215	France	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.108.154.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.138.161.1	France	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.194.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.31.202	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
185.27.105.82	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
37.26.148.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.67.24.253	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
77.139.210.106	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/eitan/pratim/pirteychayal/	Block	1
81.218.101.66	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 81.218.101.66	Block	1
45.56.107.109	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteyerua/	Block	1
79.176.31.165	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at ˆÌ·Zm[[#28]]1›fü[[#16]]ìdÛ†§r«ä&#012ìÛ²±¾à[[#15]][[#2]][[#7]]‡¢Õ&Î¤î¿•Çdªü[[#31]]Ñ¾[[#29]]fjhxµ›Ç•[“oÛ+<[[#11]]yQV[[#11]]§'PI¸#c*8•ýéB3BÞ[[#14]]™¸³cX£LX)Q…'UY[[#27]]‡@±ýÔA®jssA#012KÂÔv¼Û[[#21]]Ðßè4ýb`#rV)G–ãð[[#1]]á[§ø[[#27]][[#7]]ÞB¢óÙ(ÙõÖ÷ŽT‰»jB?5[[#6]][[#24]]¼×[[#21]]ùâ“o[[#27]][[#24]]Œ`¶n![[#24]],Þªå@[[#8]]cT®^¯Ö[[#2]]ª†Ñ¢ü}®šŒ[[#1]]´Õ¥+Ux¡^–ñ	Block	1
79.176.31.165	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version ÉÊ¥Ýä[[#30]]³Ò»=éŒ†‹É¿Ïò:Î¬ÔŸ.,JûOo£™t:-"ð[[#23]]:ÿý¥[[#14]]×Ö[[#29]]	Block	1
166.20.224.13	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
77.139.56.82	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/	Block	1
87.68.13.247	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.178.120.54	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
66.102.6.29	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
79.176.31.165	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 79.176.31.165	Block	1
31.154.19.210	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
109.253.138.119	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.176.31.165	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Multiple Malformed HTTP Header Line from 45.79.71.122	Block	1
79.176.31.165	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.176.31.165	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 79.176.31.165	Block	1
178.63.101.134	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
77.139.75.2	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/megurim/	Block	1
87.68.28.20	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
79.180.161.72	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.224	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/938-he/patzar.aspx	Block	1
37.19.121.195	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/57056.pdf&ved=0ahukewj88mpmt6fmahuc_iwkhwntar4qfggdmai&usg=afqjcnf1yolugsboijiblzxiye0gplabcg&sig2=sljt3vnb9hu32rwuqzye5w	Block	1
79.176.31.165	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 79.176.31.165	Block	1
79.176.31.165	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
77.138.249.220	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Multiple Malformed URL from 45.79.71.122	Block	1
79.176.31.165	Israel	147.237.72.166	aka.idf.il	Too Many Headers per Request - 31 Headers	Block	1
79.176.31.165	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 79.176.31.165	Block	1
184.96.96.74	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
109.66.2.210	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
77.139.179.246	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/popups/popup.aspx	Block	1
80.246.130.231	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1631-he/refuah.aspx	Block	1
37.26.147.153	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 37.26.147.153	Block	1
79.176.31.165	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 79.176.31.165	Block	1
79.176.31.165	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Parameter Value at 5 for [[#19]]ƒh[[#23]]ך[[#18]]cw¨j¸[[#19]]u.x[[#11]]3(ıשy[[\•¬#12¸m]]61#[[]]1#[[Ê[″t³]]71#[[j]]¨ק¸:žcı|]]µ¨:[[#29¸]]#31[[¡‹¿¦'ר¸"c7˜ק]]#28[[ı'8²]]#31[[	Block	1

09-07-2016-22:04:07 to 09-07-2016-23:04:07