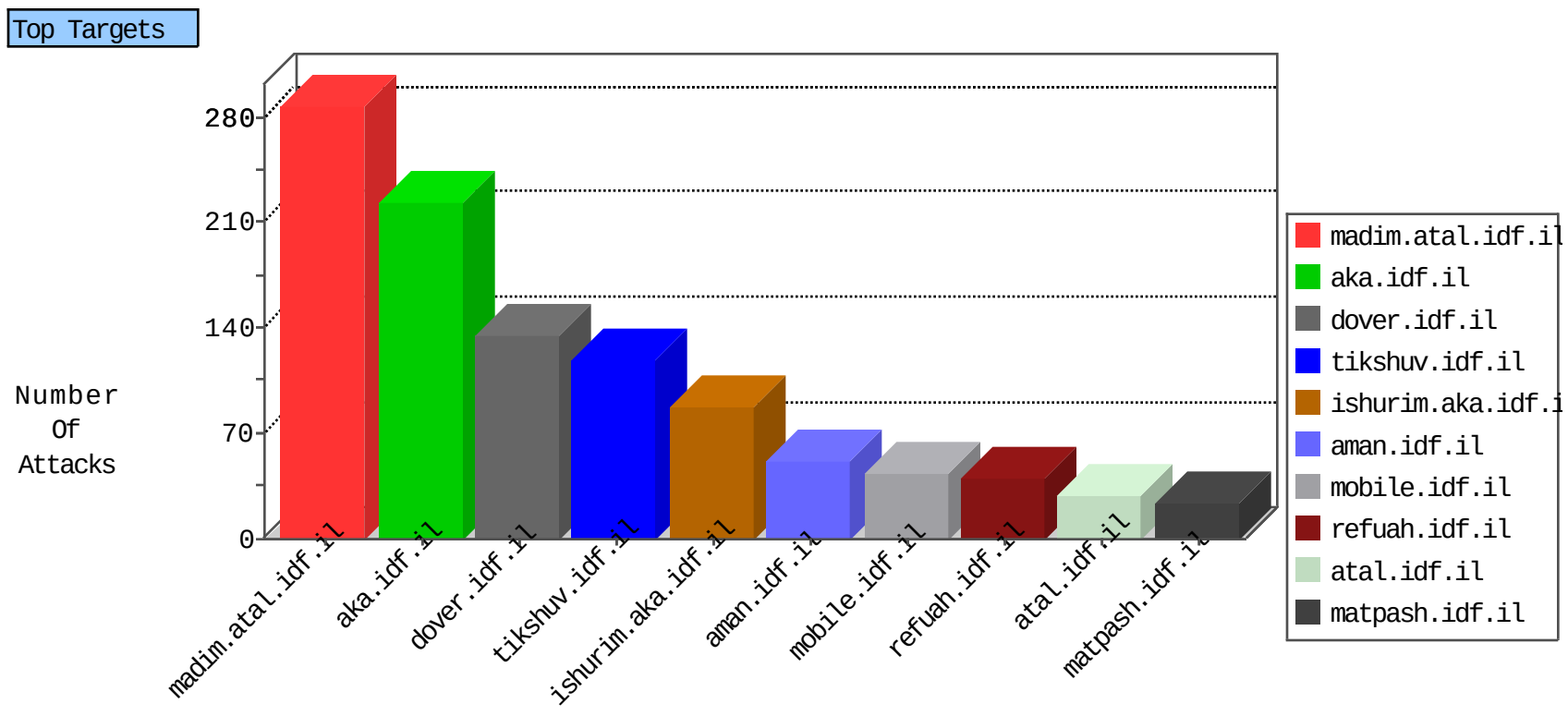
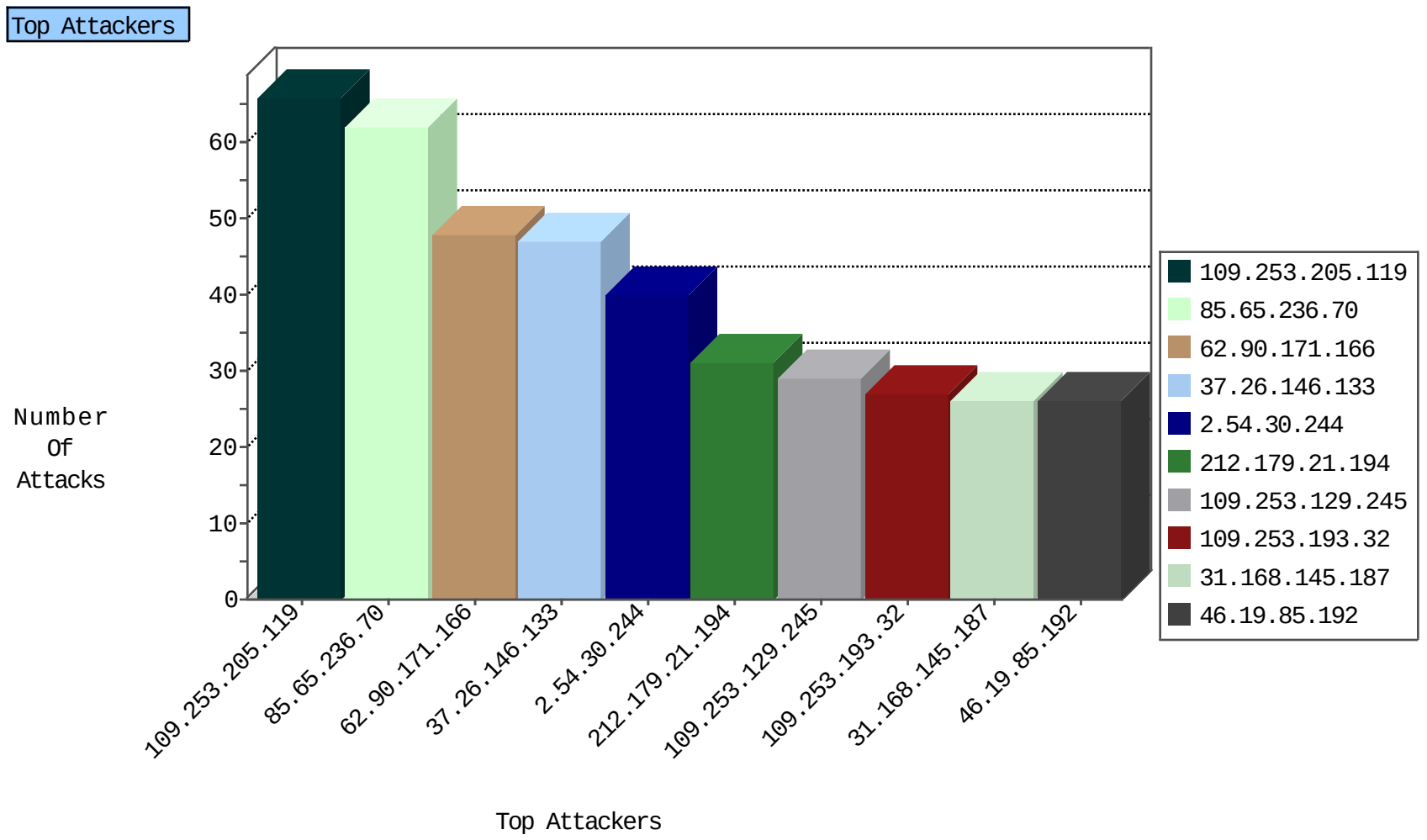
02-14-2016-13:04:01 to 02-14-2016-14:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-14-2016-13:04:01 to 02-14-2016-14:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.105.16.238	Turkey	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
93.158.203.154	Netherlands	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
112.203.9.189	Philippines	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
198.20.70.114	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

02-14-2016-13:04:01 to 02-14-2016-14:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
210.1.218.60	Australia	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

02-14-2016-13:04:01 to 02-14-2016-14:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.253.205.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
185.110.110.212	147.237.72.166		aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.69.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.136.80	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.192.6.154	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
105.226.175.208	147.237.77.121	South Africa	e.navy.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
105.226.175.208	147.237.76.196	South Africa	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
104.35.201.12	147.237.77.74	United States	law.idf.il	ET SCAN Potential SSH Scan	1
104.35.201.12	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
212.199.244.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
99.226.146.61	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
203.83.17.155	147.237.77.178	Papua New Guinea	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
87.69.26.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.34.56.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.120.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.126.16	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
105.226.175.208	147.237.77.176	South Africa	matpash.idf.il	ET SCAN Potential SSH Scan	1
46.121.246.165	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
105.226.175.208	147.237.77.61	South Africa	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
31.168.170.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
105.226.175.208	147.237.0.15	South Africa	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.35.201.12	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
104.35.201.12	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
203.83.17.155	147.237.77.178	Papua New Guinea	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
89.139.163.0	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
203.83.17.155	147.237.77.178	Papua New Guinea	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
79.183.59.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-14-2016-13:04:01 to 02-14-2016-14:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.192	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	26
31.168.145.187	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
77.125.128.90	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
31.168.185.0	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.179.142	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
80.246.130.14	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
109.160.141.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.142.68.44	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.117.124.214	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
80.246.130.14	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.54.179.142	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.151.45.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.181.148	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.200.205.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.179.142	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.86.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.94.98.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.6.108	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.129.245	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.145.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.133	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.242	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.52.168.176	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
66.102.9.125	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.80.196.44	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
91.200.12.7	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
140.194.140.63	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
159.203.123.37	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
192.240.96.68	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
87.69.185.73	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.181.128	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.193	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
109.66.207.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.170.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.135.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.5.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.12		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	3
192.115.203.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.253	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-14-2016-13:04:01 to 02-14-2016-14:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.205.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
85.65.236.70	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	62
62.90.171.166	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	48
37.26.146.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
2.54.30.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	40
109.253.193.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
109.253.129.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
2.52.137.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
176.13.6.108	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.6.108	Block	9
2.54.163.11	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
109.253.150.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
193.106.206.10	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	6
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	4
37.186.82.231	Armenia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.186.82.231	Block	4
41.202.219.65	Cameroon	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
37.186.82.231	Armenia	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 37.186.82.231	Block	4
41.202.219.65	Cameroon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	4
109.66.58.61	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.66.58.61	Block	4
5.22.130.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.146.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.3.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
95.143.172.178	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.143.172.178	Block	3
185.32.179.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.14.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.136.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.186.82.231	Armenia	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 37.186.82.231	Block	2
31.168.185.0	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1439-he/muluim.aspx	Block	2
109.64.10.137	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	2
83.130.107.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
37.26.146.224	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.6.108	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
192.115.203.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
87.69.62.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.62.227	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
79.177.129.81	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$74 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in URL y>Ã?>×´[[#6]]×›•â€?Â¯0ÂµÖ±g$	Block	1
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
201.6.229.201	Brazil	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
176.13.14.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
95.86.112.126	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-9667-he/cogat.aspx&sa=u&ved=0ahukewjzqkivl_fkahvid5okhs1yaqo4kbcqhqeinjan&sig2=vmp_wr6xitsl4viwz66riq&usg=afqjcnhvgraiolnfnkeyvoxrv2_g34qyda	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in Header Name HÃ¯[[#14]]vÂ·ÃƒÂ§[[#6]]OÂ–Â´>Cp	Block	1
80.246.136.220	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
213.151.56.160	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/3/109023.pdf&sa=u&ved=0ahukewiepj76mvfkahxk6rqkhtiqbvcqfggsmam&usg=afqjcnhaq4bgvb4nauvkclkmuqz3o9ishw	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Illegal Byte Code Character in Method Ã¢[[#11]][[#15]]Ã„#Ã´Ã°;[[#23]][[#30]]Â^Â¹UÃ„>\Â…Ã´NÂ©[[#14]]Ã™Ã”+Â^[[#4]]Â¹Ã¯	Block	1
109.66.58.61	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar	Block	1
87.69.62.227	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
31.168.185.0	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.168.185.0	Block	1
79.178.10.60	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1

02-14-2016-13:04:01 to 02-14-2016-14:04:01