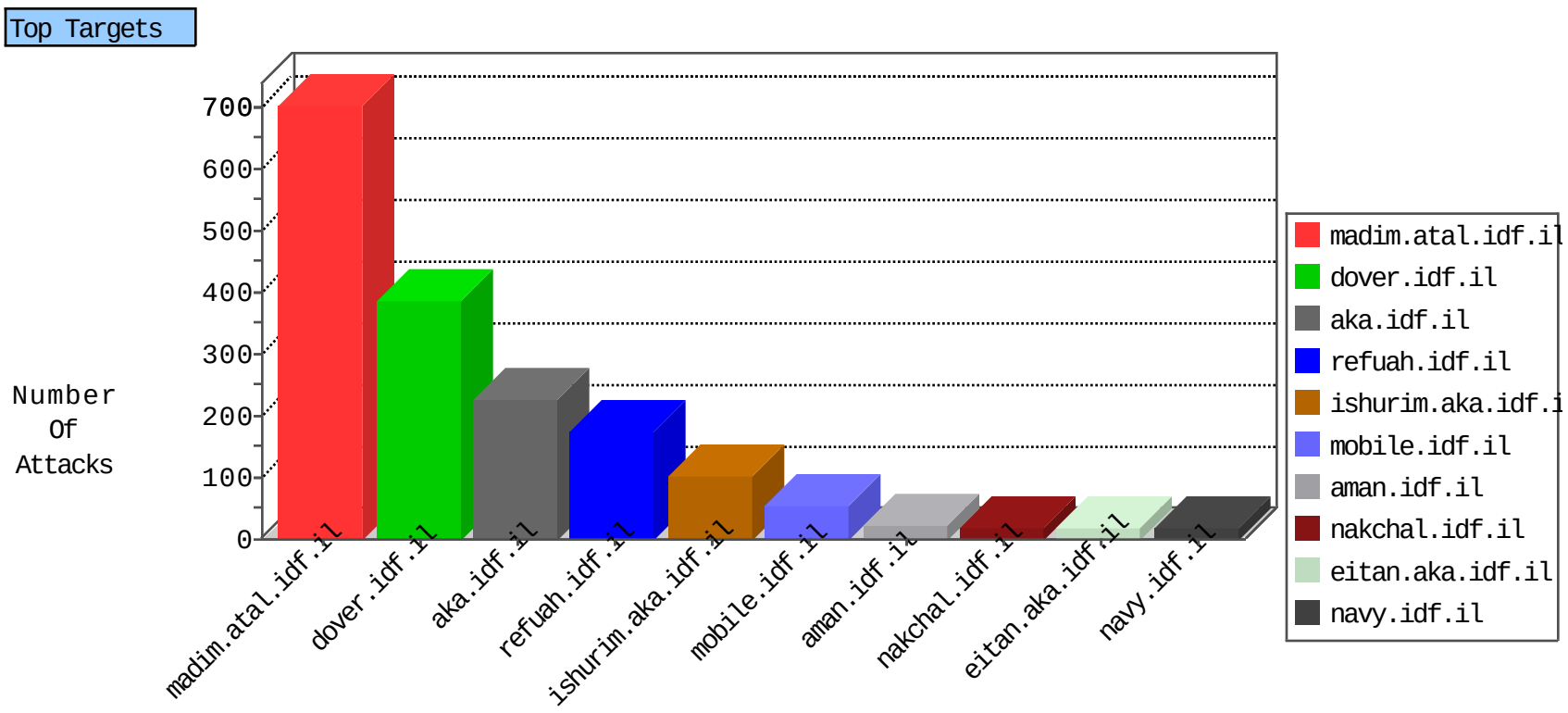
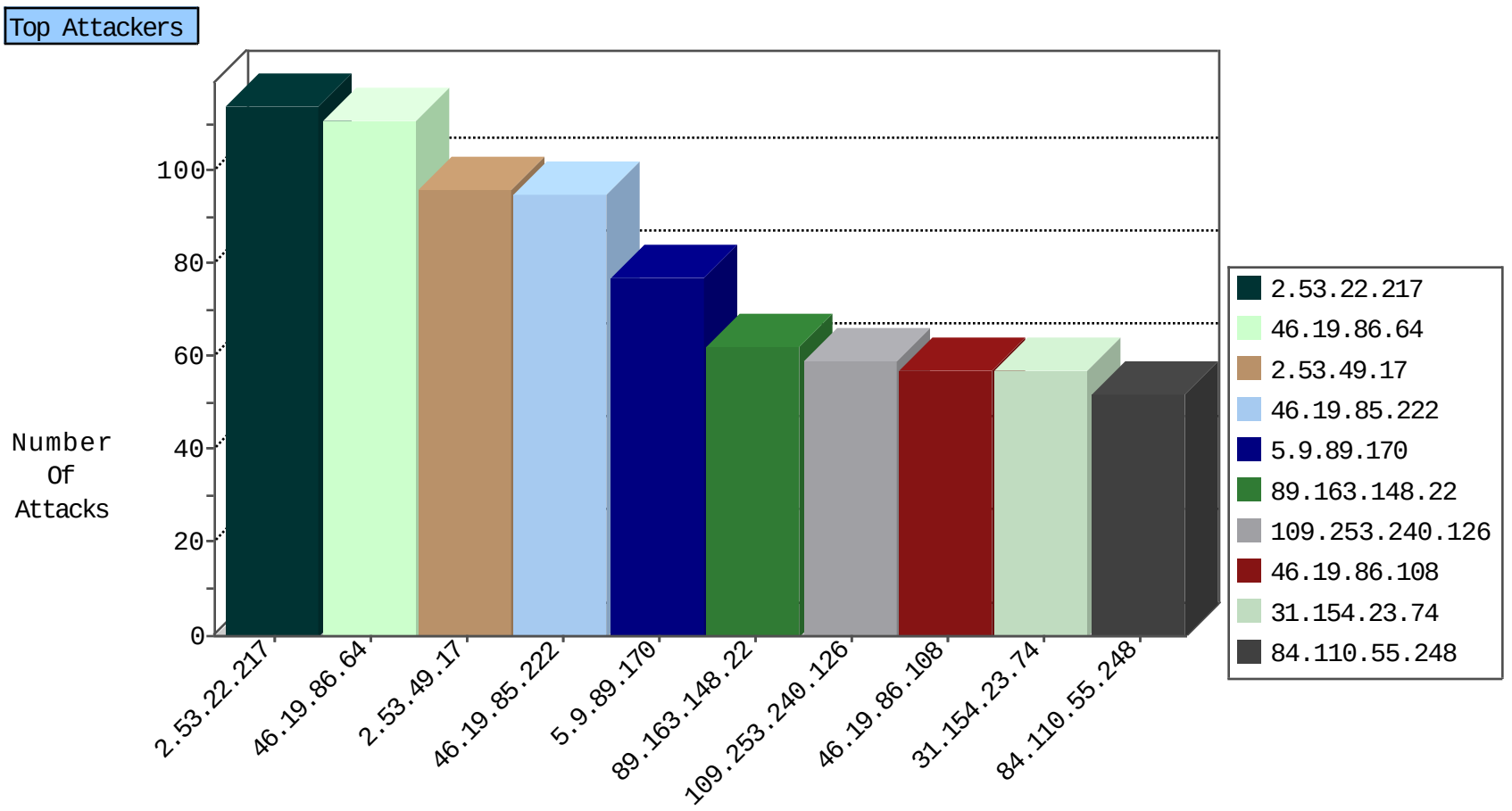
09-15-2016-10:04:02 to 09-15-2016-11:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-15-2016-10:04:02 to 09-15-2016-11:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.0.105.133	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	463
79.183.41.31	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	143
5.28.140.25	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
80.178.3.104	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.179.150.72	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
81.218.251.252	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-15-2016-10:04:02 to 09-15-2016-11:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.89.170	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	35
89.163.148.22	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	27
5.9.89.170	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	21
89.163.148.22	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	18
5.9.89.170	Germany	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	11
89.163.148.22	Germany	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	11
5.9.89.170	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	5
89.163.148.22	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	4
5.9.89.170	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	3
89.163.148.22	Germany	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Permit	2
5.9.89.170	Germany	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Permit	1
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-15-2016-10:04:02 to 09-15-2016-11:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
79.180.164.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.232.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.59.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
62.219.151.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.72.156	Ukraine	aman.idf.il	ET SCAN Potential SSH Scan	1
5.29.140.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
2.53.35.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
141.226.151.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.136.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.76.144	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	1
79.178.48.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.114.5.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.40.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.76.86	Ukraine	navy.idf.il	ET SCAN Potential SSH Scan	1
62.90.215.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
31.168.27.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1
2.54.105.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
85.250.252.225	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.95.85.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-15-2016-10:04:02 to 09-15-2016-11:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.154.23.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
84.110.55.248	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	51
62.0.210.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	34
77.125.82.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
80.178.150.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	28
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
5.28.143.14	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
116.203.77.10	India	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
46.19.85.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.86.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
46.19.85.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
46.19.86.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.86.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
46.19.86.10	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.108	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
80.178.150.219	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
46.19.85.230	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
62.0.213.1	Israel	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.230	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.108	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
194.90.66.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.138.203	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.139.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
116.203.77.10	India	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.65.99.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.154.194	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.69.212	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
49.32.56.219	India	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.139.205	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.149.150	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.19.86.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.54	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
62.0.200.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
109.253.240.112	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
176.13.14.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.54	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.108	Israel	147.237.77.216	dover.idf.il	SYN Attack		monitor	4
46.19.85.143	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.143	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

09-15-2016-10:04:02 to 09-15-2016-11:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.22.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
46.19.86.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
2.53.49.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
46.19.85.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	95
109.253.240.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
213.57.178.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
176.13.15.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
2.53.48.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
176.13.231.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
176.13.226.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
176.13.2.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
185.32.179.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
79.178.232.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
77.125.79.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
192.118.12.102	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	4
81.218.251.250	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	4
81.218.37.2	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 81.218.37.2	Block	4
81.218.37.2	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.37.2	Block	4
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 199.203.215.1	Block	3
192.118.12.102	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.12.102	Block	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
2.53.184.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.71.40.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
109.226.48.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtFirstName in madim.atal.idf.il/1088-he/meretz.aspx	Block	2
46.19.85.108	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
192.114.5.10	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
2.55.18.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
81.218.251.250	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	2
37.26.149.152	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.26.149.152	Block	2
217.194.207.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
46.19.86.184	Israel	147.237.77.74	law.idf.il	Illegal HTTP Version __atuvs=57da487d74ea1ff0000	Block	1
81.218.251.252	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
37.26.149.170	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	NULL Character in URL	Block	1
80.246.130.8	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
66.249.64.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/61267.gif	Block	1
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/back.png	Block	1
5.28.143.14	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method là÷è@É[[#16]]>_Zýê“[[#31]][[#8]][[#23]]<½¡š¥Ñ÷lfu£^ÓjÊ£ÀïÑÙõY-Û in URL	Block	1
77.138.175.19	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/rights/asp/info.asp	Block	1
157.55.39.202	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/tizmoret/gallery/	None	1
46.19.86.184	Israel	147.237.77.74	law.idf.il	Malformed URL __atuvc=1	Block	1
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/sachar/	Block	1

09-15-2016-10:04:02 to 09-15-2016-11:04:02