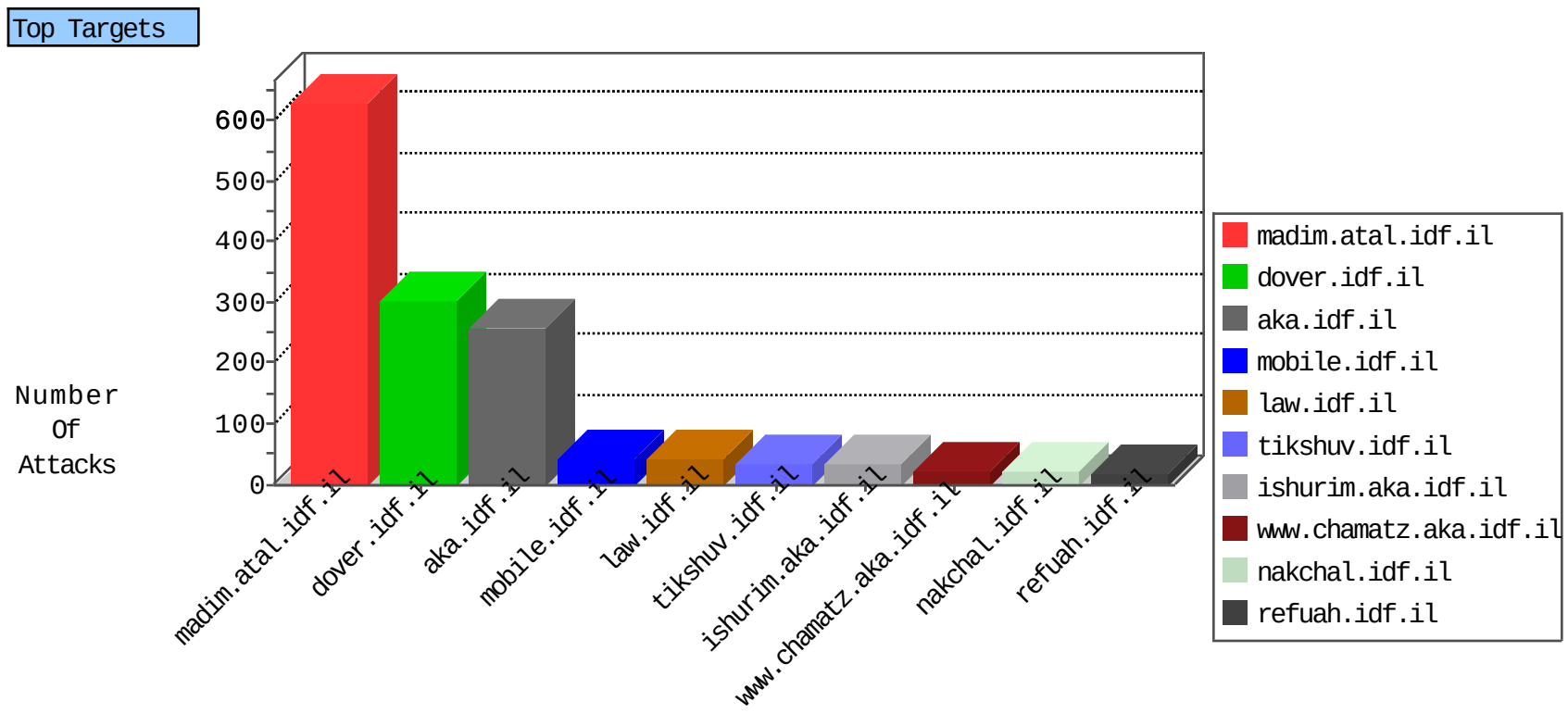
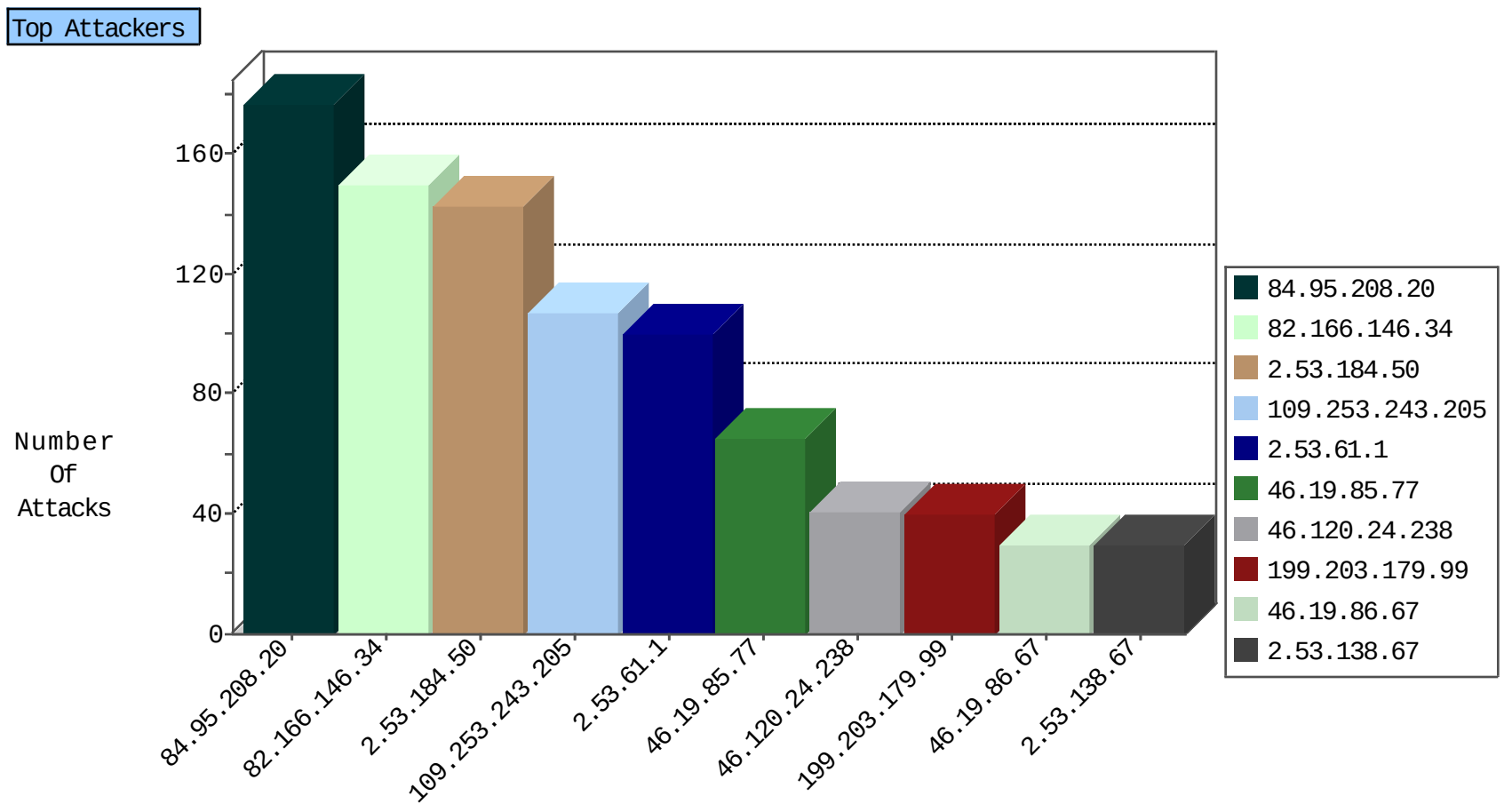
09-19-2016-10:04:08 to 09-19-2016-11:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-19-2016-10:04:08 to 09-19-2016-11:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.18.52	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
2.55.62.238	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
165.242.90.128	Japan	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
77.138.224.25	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
173.208.197.206	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
63.141.242.197	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
173.208.150.117	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.68	Switzerland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
69.30.193.252	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	1
173.208.197.203	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
69.30.226.218	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
173.208.197.205	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1

09-19-2016-10:04:08 to 09-19-2016-11:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.74	United States	147.237.76.176	test.ncore.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-19-2016-10:04:08 to 09-19-2016-11:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.229.0.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.245.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.139.166.125	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.81.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.162.105.152	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	1
5.22.134.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.47.165.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.45.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
154.16.199.175	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
82.166.204.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.140.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.75.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.28.181.69	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.163.56	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.167.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

09-19-2016-10:04:08 to 09-19-2016-11:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
2.53.138.67	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
199.203.179.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
62.0.200.125	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	27
84.52.98.134	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
109.253.213.202	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
62.0.251.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
46.120.24.238	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
2.53.163.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.217.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.120.24.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	12
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.97	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
85.250.59.223	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
176.13.15.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.120.24.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
82.166.198.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.150.37.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
213.57.127.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.120.24.238	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
2.53.166.254	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
82.80.196.44	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
80.178.204.62	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.55.12.150	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.67	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.0.222.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
199.203.179.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.67	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.46.38.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.22.134.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.67	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.95	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.67	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
88.202.218.237	United Kingdom	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.130.217.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.203.179.99	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	4
109.253.243.205	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	4
62.0.221.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
176.13.15.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
156.212.86.66	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
80.178.101.40	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.121	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.111.234.11	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.26.148.166	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
109.253.243.205	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
176.13.248.233	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
176.13.5.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
199.203.179.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2

09-19-2016-10:04:08 to 09-19-2016-11:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.166.146.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	150
2.53.184.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	143
2.53.61.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
109.253.243.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	99
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	73
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	67
46.19.85.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.85.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	15
62.219.130.248	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	10
2.53.55.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
109.65.92.78	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized HTTP Method	Block	5
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	4
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	3
80.246.137.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.179.21.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/	Block	3
212.150.71.177	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
46.19.86.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	2
212.25.84.200	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
85.64.18.29	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.53.25.139	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
198.21.92.122	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2016/lobby.aspx	Block	2
46.19.86.12	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
37.26.149.175	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
217.194.207.24	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.40	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
66.249.66.234	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/לכתבה המלאה	Block	1
87.68.35.145	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.86.34	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
77.138.229.21	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.229.21	Block	1
46.117.232.79	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.253.243.212	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl67 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.86.12	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvs=57df939e3eae38d0000; _pk_ref.20.8afc=%5B%22%22%2C%22%22%2C1474270112%2C%22http%3A%2F%2Fwww.google.co.il%2F%22%5D; _pk_id.20.8afc=8314f6d8a508ff48.1474270112.1.1474270112.1474270112.; _pk_ses.20.8afc=*	Block	1
82.81.160.69	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.85.38	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
207.46.13.148	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/894-en	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.70	Block	1
77.138.229.21	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
212.150.71.177	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
52.30.171.229	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	1
157.55.39.0	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in aka.idf.il/main/giyus/	None	1
46.19.86.12	Israel	147.237.77.216	dover.idf.il	Malformed URL __atuvc=1	Block	1
46.19.85.38	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/apple-app-site-association	Block	1

09-19-2016-10:04:08 to 09-19-2016-11:04:08