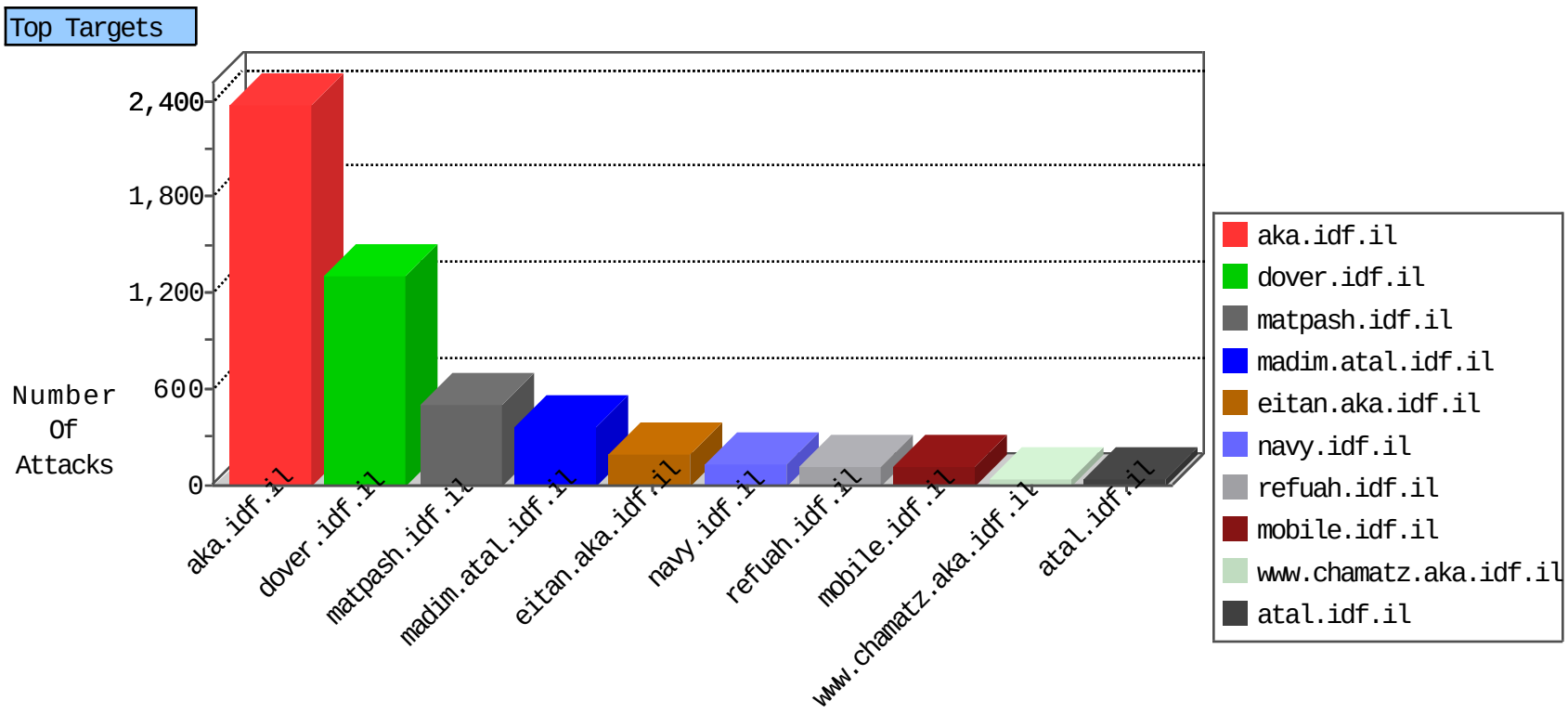
10-01-2016-19:04:08 to 10-01-2016-20:04:08

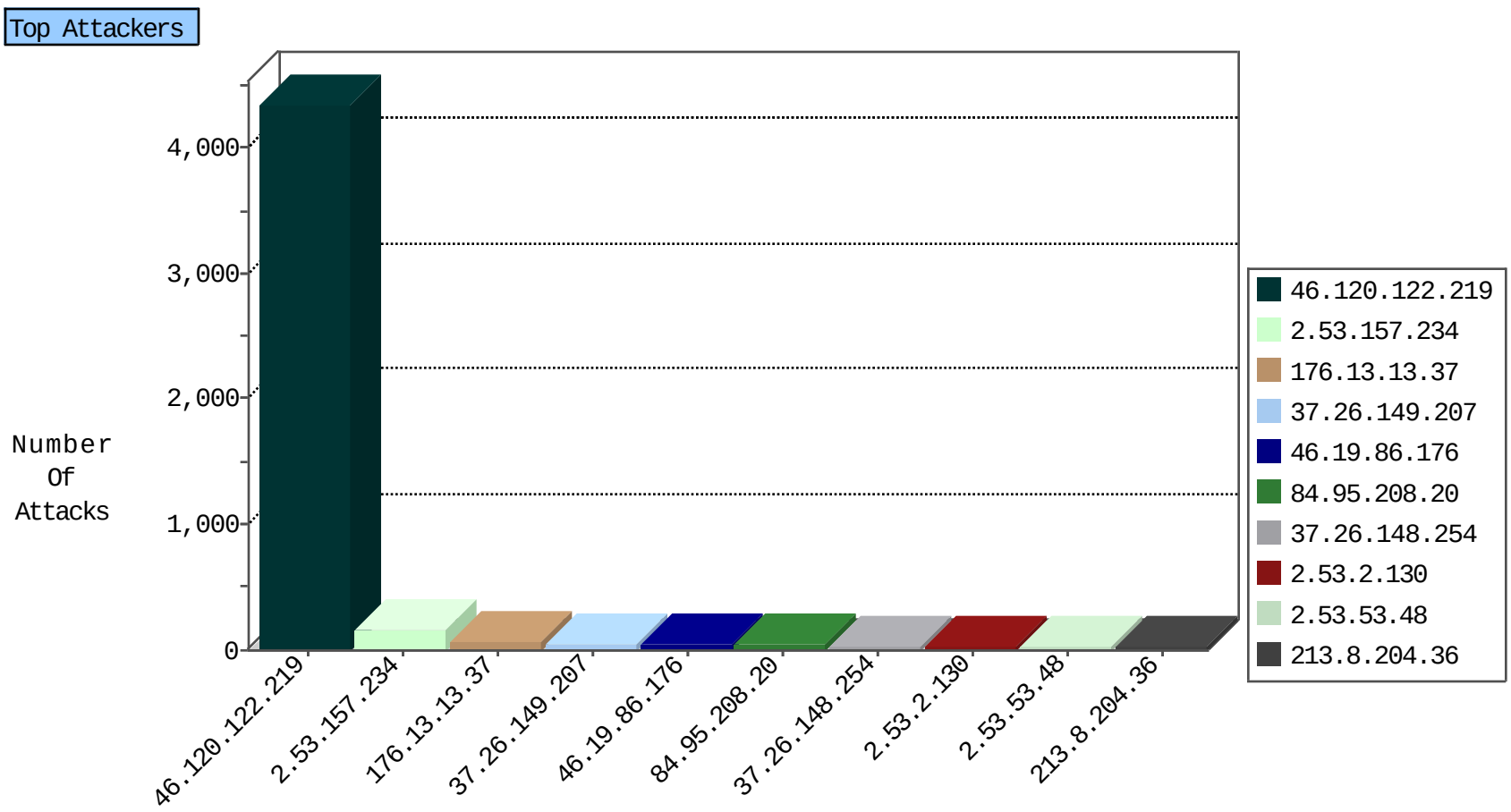
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-01-2016-19:04:08 to 10-01-2016-20:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.94.111.1	Russian Federation	147.237.76.198	e.yohalan.idf.il	Black List	drop	1

10-01-2016-19:04:08 to 10-01-2016-20:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.91.70.94	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6

10-01-2016-19:04:08 to 10-01-2016-20:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	1270
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	1121
46.120.122.219	147.237.77.176	Israel	matpash.idf.il	Xenu Link Sleuth User Agent	454
46.120.122.219	147.237.76.200	Israel	eitan.aka.idf.il	Xenu Link Sleuth User Agent	153
46.120.122.219	147.237.76.86	Israel	navy.idf.il	Xenu Link Sleuth User Agent	126
46.120.122.219	147.237.76.42	Israel	refuah.idf.il	Xenu Link Sleuth User Agent	93
46.120.122.219	147.237.0.34	Israel	tikshuv.idf.il	Xenu Link Sleuth User Agent	20
23.91.70.94	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	14
46.120.122.219	147.237.76.31	Israel	nakchal.idf.il	Xenu Link Sleuth User Agent	8
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	6
46.120.122.219	147.237.77.233	Israel	atal.idf.il	Xenu Link Sleuth User Agent	6
46.120.122.219	147.237.0.15	Israel	kosher-kravi.idf.il	Xenu Link Sleuth User Agent	4
46.120.122.219	147.237.77.226	Israel	www.chamatz.aka.idf.il	Xenu Link Sleuth User Agent	2
14.152.59.11	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.76.200	United Kingdom	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.82.44	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.222.5	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.163.3	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
201.114.60.162	147.237.0.16	Mexico	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.163.3	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
41.215.36.46	147.237.77.212	Kenya	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
188.225.38.173	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.217	147.237.77.176	Europe	matpash.idf.il	ET SCAN NMAP -sA (2)	1
40.114.15.49	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.177	China	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
64.233.172.139	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
183.60.48.25	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.76.199	United Kingdom	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.222.5	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
112.66.60.114	147.237.77.121	China	e.navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
201.114.60.162	147.237.0.16	Mexico	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
89.248.163.3	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
188.225.38.173	147.237.77.74	Russian Federation	law.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.163.3	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
41.215.36.46	147.237.77.74	Kenya	law.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.65.51	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
40.114.15.49	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

10-01-2016-19:04:08 to 10-01-2016-20:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.2.130	Israel	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
2.53.53.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
213.8.204.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.120.122.219	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
185.27.105.76	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.148.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
185.7.121.20	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
85.64.185.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.190.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.120.122.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
37.26.148.254	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
37.26.148.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.149.235	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
31.10.155.190	Switzerland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
141.226.232.17	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
37.26.149.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.222	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.139.234.223	France	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
176.13.8.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.120.122.219	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
37.26.149.235	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.8.107.93	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.120.122.219	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.86.70	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.120.122.219	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
37.26.148.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.138.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.138.69	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.138.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.149.235	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.174	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.172	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.176.97.188	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	4
46.120.122.219	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.120.122.219	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
89.46.176.172	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.78	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.226.218.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.179.116.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.181.99.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.27.105.106	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.32.179.118	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
85.64.185.173	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
130.255.69.186	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

10-01-2016-19:04:08 to 10-01-2016-20:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	995
2.53.157.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	144
176.13.13.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
37.26.149.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
46.19.86.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
2.53.157.234	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	14
37.26.149.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
46.120.122.219	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 46.120.122.219	Block	12
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.122.219	Block	11
46.210.240.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.55.32.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	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
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
46.120.122.219	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.120.122.219	Block	5
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
46.117.187.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.27.105.76	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
77.138.109.213	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.175.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
79.181.139.55	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
2.55.159.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.176.97.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	1
188.120.154.189	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
41.45.109.247	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	1
77.138.121.222	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/kiosk/printablekiosk.aspx	Block	1
176.13.8.175	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
23.250.3.10	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.65.143	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.charts.js	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/null	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
46.19.85.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.139.237	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotfaq.aspx	Block	1
176.13.8.175	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.230.186	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
84.229.65.131	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
46.120.122.219	Israel	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/894-he/refuah.aspx	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
46.19.85.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.11.127	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/main/home/default.aspx	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
77.138.69.32	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	1

10-01-2016-19:04:08 to 10-01-2016-20:04:08