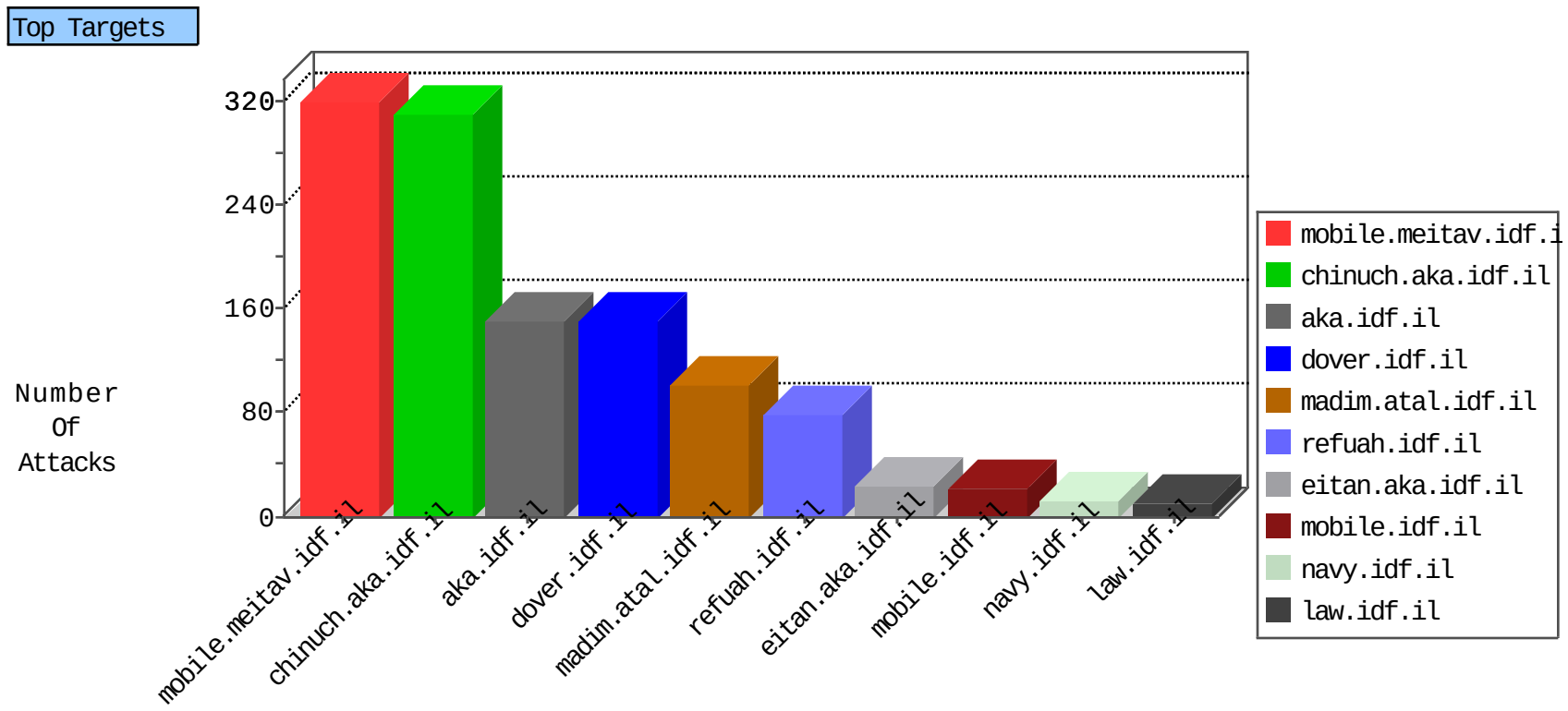
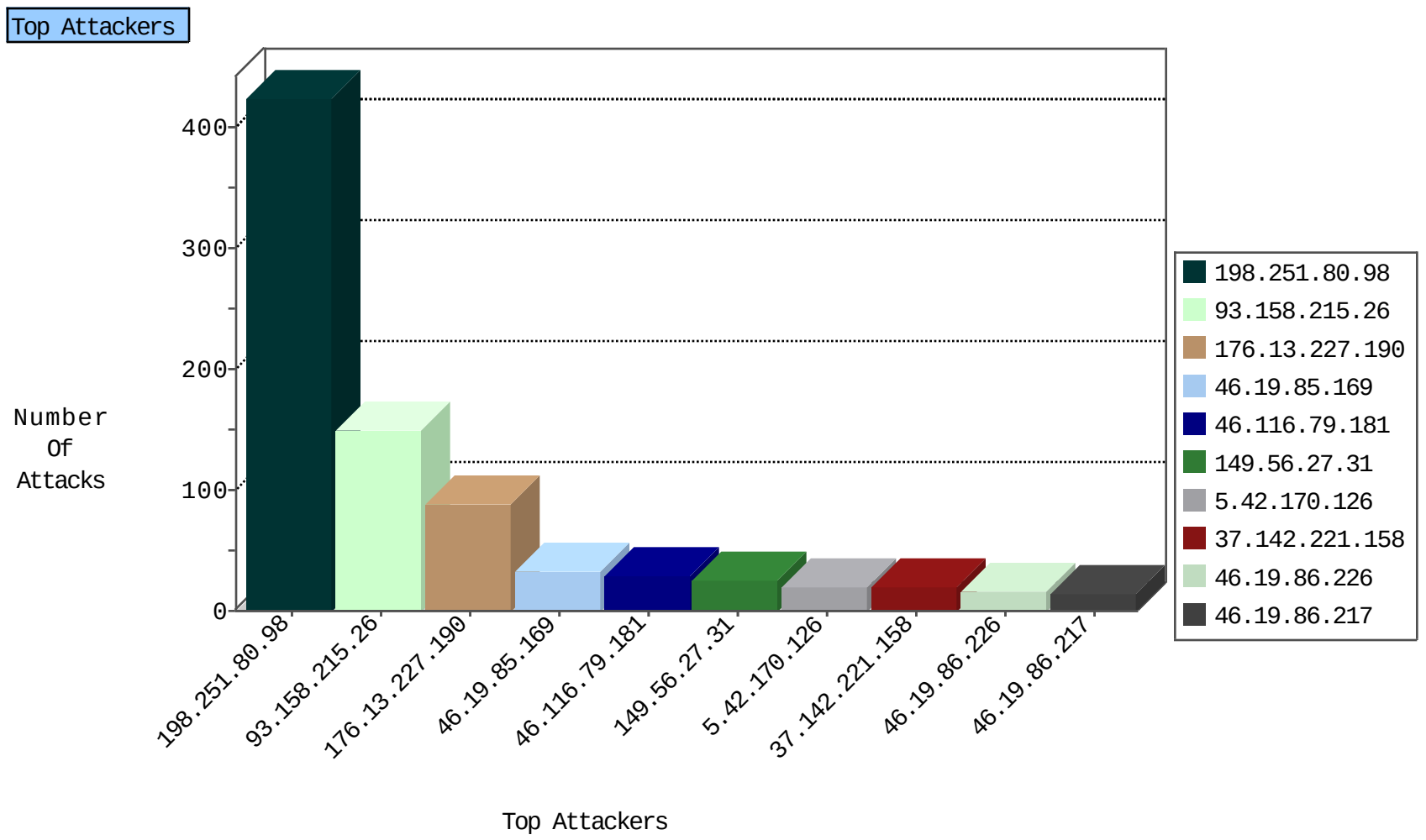
09-25-2016-22:04:03 to 09-25-2016-23:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-25-2016-22:04:03 to 09-25-2016-23:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.193.178	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
77.127.13.121	Israel	147.237.76.42	refuah.idf.il	Black List	drop	3
46.120.173.120	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
141.212.122.135	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	1
84.229.30.108	Israel	147.237.76.42	refuah.idf.il	Black List	drop	1
180.97.106.162	China	147.237.76.201	e.atal.idf.il	Black List	drop	1
93.174.94.235	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
123.59.59.52	China	147.237.77.74	law.idf.il	block-sp-traf1	forward	1

09-25-2016-22:04:03 to 09-25-2016-23:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.217.24	Israel	147.237.72.156	aman.idf.il	32390: HTTP: Suspicious User-Agent (Mozilla)	Block	2
123.126.68.119	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-25-2016-22:04:03 to 09-25-2016-23:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
105.103.45.72	147.237.76.42	Algeria	refuah.idf.il	ET SCAN Potential SSH Scan	2
105.103.45.72	147.237.76.148	Algeria	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
94.74.129.245	147.237.76.42	Iran, Islamic Republic of	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.160.198	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
86.124.67.56	147.237.8.46	Romania	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
191.96.249.189	147.237.77.121	Chile	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.14.11	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
105.103.45.72	147.237.76.202	Algeria	e.halag.idf.il	ET SCAN Potential SSH Scan	1
62.150.255.205	147.237.76.177	Kuwait	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
105.103.45.72	147.237.76.198	Algeria	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
105.103.45.72	147.237.76.196	Algeria	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential VNC Scan 5800-5820	1
105.103.45.72	147.237.76.176	Algeria	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
41.215.36.46	147.237.77.212	Kenya	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
93.168.20.23	147.237.77.176	Saudi Arabia	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
89.39.74.45	147.237.76.34	Romania	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
209.95.50.84	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
84.94.198.81	147.237.76.147	Israel	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
106.187.45.144	147.237.77.178	Japan	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
62.150.255.205	147.237.76.177	Kuwait	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
105.103.45.72	147.237.76.201	Algeria	e.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
105.103.45.72	147.237.76.197	Algeria	e.himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
105.103.45.72	147.237.76.177	Algeria	ncore.idf.il	ET SCAN Potential SSH Scan	1
41.215.36.46	147.237.77.226	Kenya	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1

09-25-2016-22:04:03 to 09-25-2016-23:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
93.158.215.26	Netherlands	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	60
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	47
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	47
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	46
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	46
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	44
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	Invalid ACK number	monitor	44
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	43
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	39
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	37
93.158.215.26	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	36
93.158.215.26	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack		monitor	35
46.19.85.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	32
37.142.221.158	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
93.158.215.26	Netherlands	147.237.76.39	mobile.meitav.idf.i	SYN Attack		monitor	15
149.56.27.31	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
2.54.96.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
84.94.184.21	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
77.126.33.217	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.56.27.31	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
2.53.172.136	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
80.178.170.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.116.79.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.217	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.116.79.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
84.111.188.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.86.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.54.215	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.111.188.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
176.67.58.254	Palestinian Territory Occupied	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.226	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
66.26.85.44	United States	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.116.79.181	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.69	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.116.79.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.69	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.116.79.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.149.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
93.158.215.26	Netherlands	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.177.14.11	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
109.253.220.40	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
149.56.27.31	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
66.249.64.85	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

09-25-2016-22:04:03 to 09-25-2016-23:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.227.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
185.120.126.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.10.5	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
79.181.10.1	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 79.181.10.1	Block	3
77.138.237.170	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	2
46.19.85.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
77.139.65.74	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	2
46.19.86.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.64.249.107	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/guyus	Block	2
2.53.174.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.65.112.192	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
77.138.130.200	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	2
5.22.134.110	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
79.180.22.172	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.66.173	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
87.69.0.221	Israel	147.237.77.234	halag.idf.il	Parameter Type Violation search in www.logistics.atal.idf.il/1213-he/halag.aspx	Block	1
84.94.184.21	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
37.142.221.158	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
185.89.217.235	Netherlands	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
5.29.137.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
148.251.192.100	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
66.249.76.67	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/m/	Block	1
46.19.86.25	Israel	147.237.76.86	navy.idf.il	Unknown HTTP Request Method ccept-Language: in URL he-li,he-il	Block	1
84.109.214.7	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
31.154.81.74	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
79.180.118.107	Israel	147.237.72.166	aka.idf.il	Unauthorized Request Content Type from 79.180.118.107	Block	1
67.19.79.218	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /robots.txt	Block	1
89.138.111.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl07.y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.66.209	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/mobile/	Block	1
84.108.87.238	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
8.39.233.94	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
164.138.112.248	Israel	147.237.72.166	aka.idf.il	Unknown Parameter x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.111.206.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.147.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
176.13.14.35	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl25 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
89.138.111.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl12.y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.69.182	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/homepage/homepage.aspx	Block	1
84.108.87.238	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/wp-login.php	Block	1
31.154.81.74	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
77.139.255.88	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.76.85	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8746-he/refuah.aspx	Block	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	1
79.181.10.1	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method undefined in URL www.aka.idf.il/main/giyus/api/api/professiondescription/:id	Block	1
37.26.149.167	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	1
77.138.32.171	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx	Block	1
89.138.111.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl16.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1

09-25-2016-22:04:03 to 09-25-2016-23:04:03