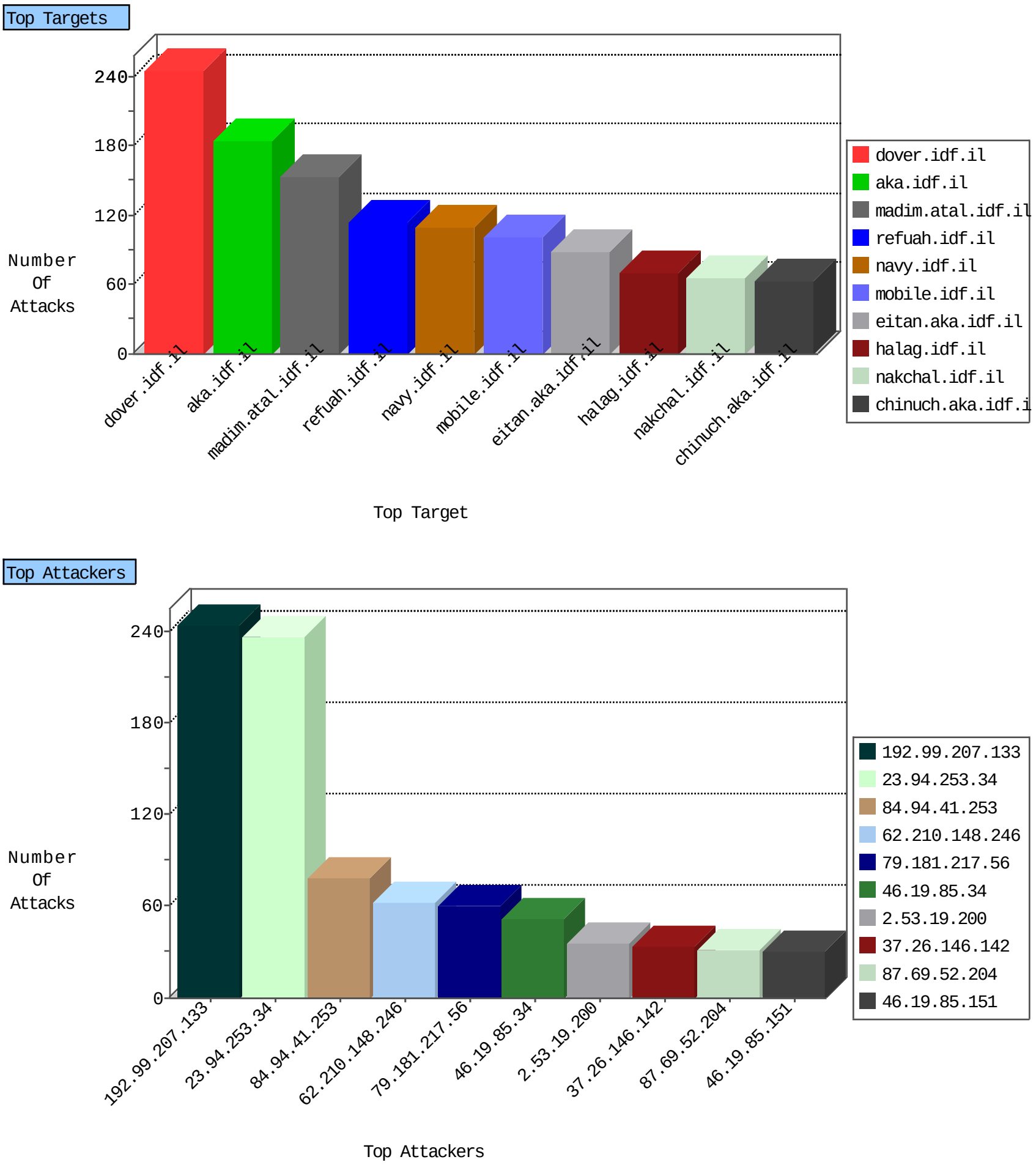
09-08-2016-20:04:08 to 09-08-2016-21:04:08

IDF Under Attack Daily Report



09-08-2016-20:04:08 to 09-08-2016-21:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
156.205.14.33	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
94.102.60.21	Netherlands	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
46.117.65.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.182.137.182	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
142.4.108.129	United States	147.237.76.201	e.atal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
89.187.217.74	Lebanon	147.237.76.30	himush.idf.il	L4 Source or Dest Port Zero	drop	1
94.177.164.99	Romania	147.237.76.201	e.atal.idf.il	Black List	drop	1

09-08-2016-20:04:08 to 09-08-2016-21:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.148.246	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	30
62.210.148.246	France	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	23
62.210.148.246	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	10
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-08-2016-20:04:08 to 09-08-2016-21:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.121.143.113	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
91.121.142.227	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
79.181.136.76	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	2
69.164.205.7	147.237.76.31	United States	nakchal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
104.128.144.131	147.237.76.44	Canada	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
66.249.93.216	147.237.77.176	Europe	matpash.idf.il	ET SCAN NMAP -sA (2)	1
66.249.93.135	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	1
180.97.106.162	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.37	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
2.50.168.178	147.237.0.35	United Arab Emirates	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
111.91.148.22	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.50.168.178	147.237.0.35	United Arab Emirates	akaws.idf.il	ET SCAN NMAP -f -sS	1
104.128.144.131	147.237.76.44	Canada	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
80.246.137.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.137	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	1
195.88.208.193	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.85	147.237.77.216	Europe	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.37	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.156	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.37	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
2.50.168.178	147.237.0.35	United Arab Emirates	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
106.186.20.183	147.237.76.198	Japan	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1

09-08-2016-20:04:08 to 09-08-2016-21:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.94.41.253	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	69
2.53.19.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
192.99.207.133	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	32
192.99.207.133	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	30
23.94.253.34	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	30
23.94.253.34	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	30
192.99.207.133	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	30
192.99.207.133	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	30
192.99.207.133	Canada	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	30
23.94.253.34	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	30
23.94.253.34	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	30
23.94.253.34	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	30
23.94.253.34	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	30
192.99.207.133	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	29
192.99.207.133	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	29
23.94.253.34	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	29
192.99.207.133	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	29
23.94.253.34	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	28
87.69.52.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
213.57.154.155	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	16
87.69.52.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
77.127.17.151	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.86.117	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
82.81.142.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
80.246.139.70	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.94.41.253	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.253.241.29	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
37.26.147.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.173.179.126	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
87.70.37.34	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
2.55.132.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.169	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
139.162.180.203	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
87.70.37.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.253.241.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
87.69.79.16	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
77.138.231.224	France	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
109.253.230.198	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.111.184.162	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
84.111.196.226	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
54.199.189.225	Japan	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
109.253.230.198	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.66.124.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
65.55.210.80	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

09-08-2016-20:04:08 to 09-08-2016-21:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.217.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
46.19.85.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
37.26.146.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
37.26.146.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
77.139.92.16	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	8
109.253.243.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
2.55.132.20	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	4
79.179.169.135	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 79.179.169.135	Block	2
80.246.137.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.108.43.72	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
80.246.139.70	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.178.105.75	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	2
37.26.147.160	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.94.41.253	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Unknown Parameter cat in www.aka.idf.il/giyus/general/	None	1
95.110.194.252	Italy	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/wp-login.php	Block	1
172.56.29.94	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
79.180.114.188	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.64.228	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	1
109.66.141.63	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
79.178.105.75	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 79.178.105.75	Block	1
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
176.13.249.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.64.184.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
24.90.141.158	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
69.164.205.7	United States	147.237.76.31	nakchal.idf.il	Multiple Untraceable SSL Sessions from 69.164.205.7 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
2.53.61.124	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.139.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.69	Block	1
204.79.180.0	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx	Block	1
89.237.68.84	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
31.154.81.61	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
80.147.219.146	Germany	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
69.164.205.7	United States	147.237.76.31	nakchal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
136.243.67.234	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
2.55.132.20	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
81.218.183.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.105.75	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/0/	Block	1
66.249.64.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20329-he/dover.aspx	Block	1
95.110.194.252	Italy	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	1
31.168.208.38	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$LoginControl$captcha$captchaText in www.aka.idf.il/main/giyus/default.aspx	None	1
80.178.208.189	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.124.21.210	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
37.46.41.156	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
144.76.16.162	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1

09-08-2016-20:04:08 to 09-08-2016-21:04:08