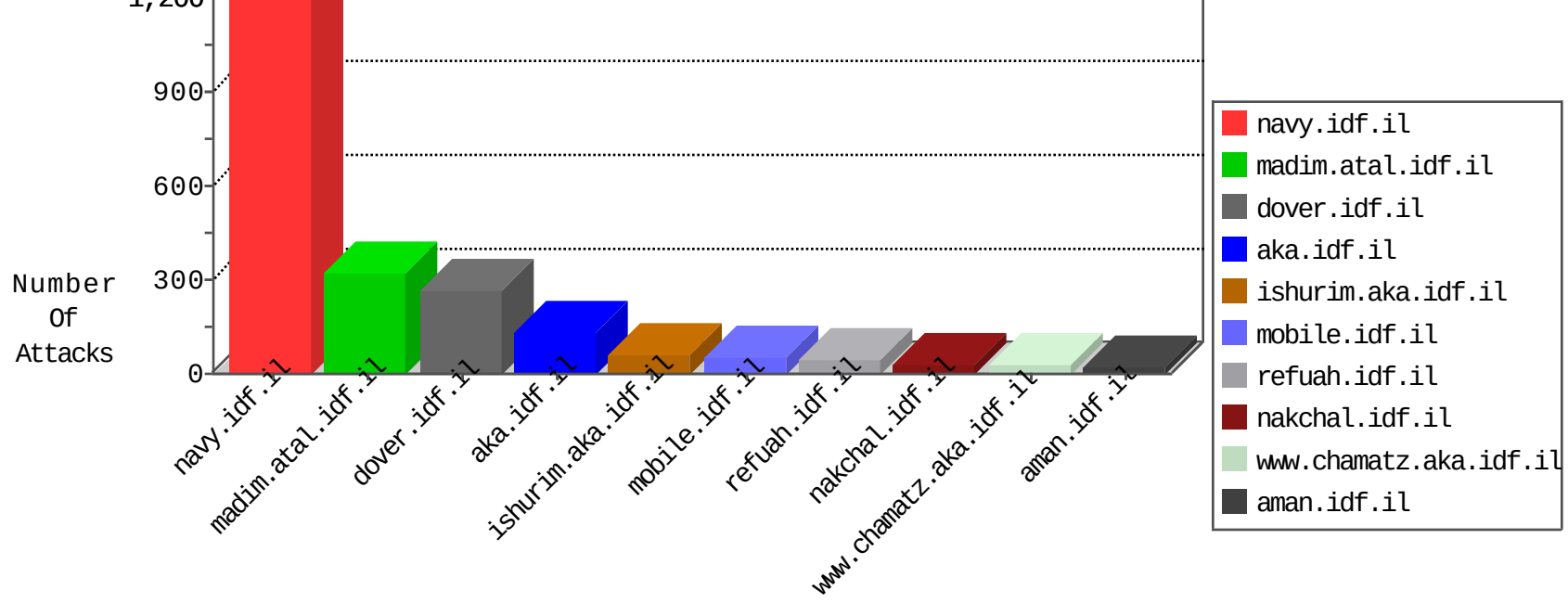
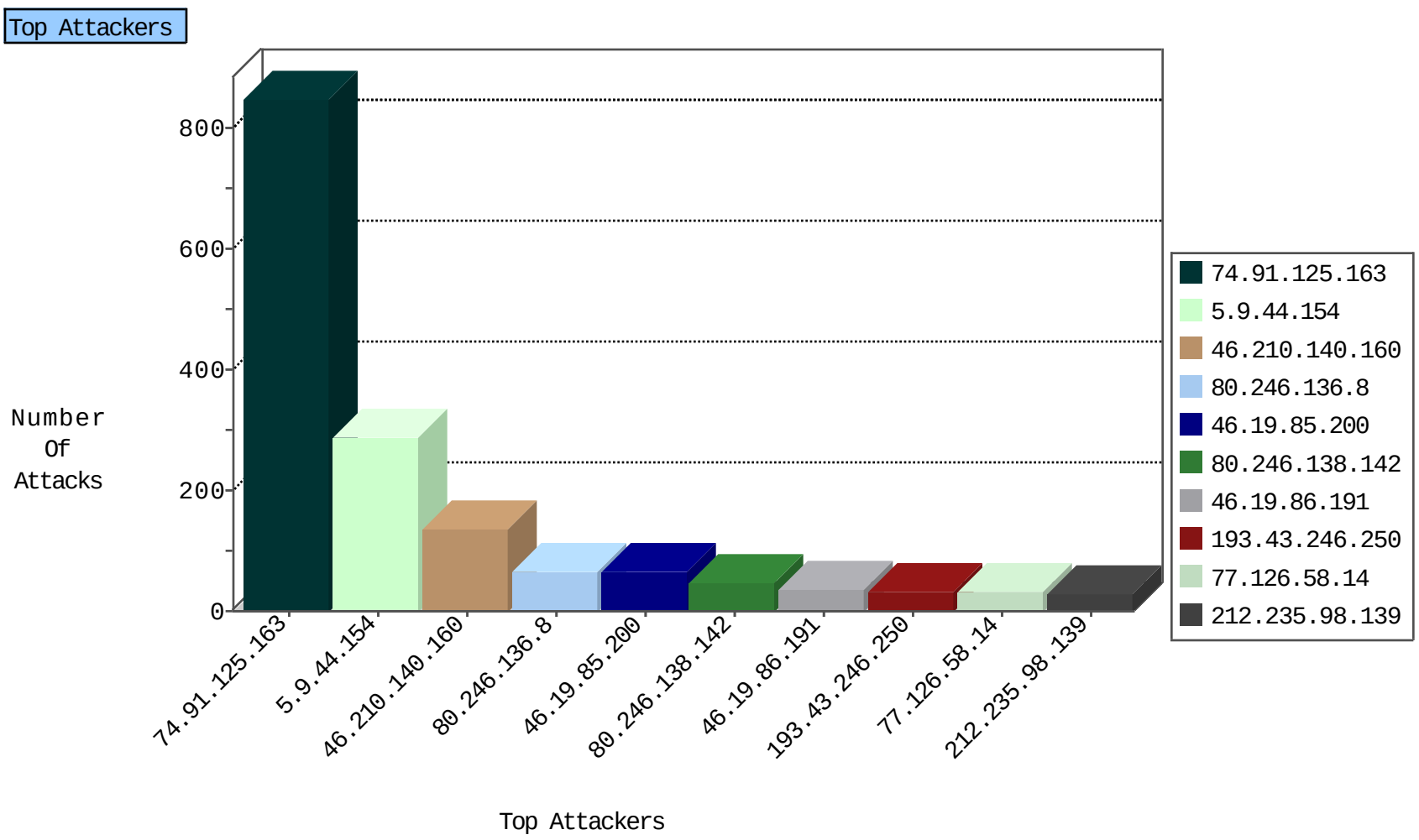
09-22-2016-15:04:09 to 09-22-2016-16:04:09

IDF Under Attack Daily Report





09-22-2016-15:04:09 to 09-22-2016-16:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.204.242	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
176.13.245.71	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
46.19.85.58	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
185.81.157.161	France	147.237.76.42	refuah.idf.il	Black List	drop	1
91.224.160.106	Netherlands	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
191.96.249.34	Chile	147.237.76.201	e.atal.idf.il	Black List	drop	1
141.212.122.28	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
191.96.249.37	Chile	147.237.76.201	e.atal.idf.il	Black List	drop	1
198.80.151.87	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

09-22-2016-15:04:09 to 09-22-2016-16:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
136.243.152.18	Germany	147.237.77.216	dover.idf.i	C1000074: HTTP: majestic bot	Permit	2
85.106.60.106	Turkey	147.237.72.166	aka.idf.il	C1000016: HTTP: administrator in URI	Permit	1
85.106.60.106	Turkey	147.237.72.166	aka.idf.il	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1

09-22-2016-15:04:09 to 09-22-2016-16:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.195.117.16	147.237.77.176	Netherlands	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
79.183.88.112	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.98.64	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
221.210.200.245	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
77.139.237.125	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
221.210.200.245	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
66.240.213.93	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.197.232.2	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN Potential SSH Scan	1
213.8.124.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.102.8.155	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
91.197.232.2	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN Potential SSH Scan	1
46.116.105.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.140.105.183	147.237.77.216	Greece	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.190.28	147.237.76.147	Hong Kong	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.243.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.190.28	147.237.76.34	Hong Kong	yohalan.idf.il	ET SCAN Potential SSH Scan	1
202.65.138.2	147.237.76.39	India	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
2.55.154.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.3.147.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.112.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.152.80.48	147.237.72.156	Switzerland	aman.idf.il	ET SCAN NMAP -sS window 4096	1
79.181.35.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
221.210.200.245	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
91.224.160.106	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
213.57.153.22	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.240.213.93	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
91.197.232.2	147.237.72.167	Russian Federation	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
62.90.96.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.109.63	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.197.232.2	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.180.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.195.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.190.28	147.237.76.38	Hong Kong	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
211.149.219.167	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
88.202.218.236	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.247.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.66.15	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.114.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
101.182.19.68	147.237.77.216	Australia	dover.idf.il	ET SCAN NMAP -sS window 4096	1

09-22-2016-15:04:09 to 09-22-2016-16:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
74.91.125.163	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	849
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	286
46.19.85.200	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.85.121	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
158.169.40.9	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.41	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.86.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.167	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.86.167	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.40	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
193.43.246.250	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
155.254.239.249	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.85.41	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.200	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.136.8	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.204.30	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.136.30	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.53.13.7	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.188	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.66	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.174	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.49.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.200	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.225	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.225	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.174	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
94.230.86.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
205.209.185.47	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
85.130.216.49	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
205.209.185.47	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.234	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
131.253.25.227	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.115.85.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
212.199.121.158	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.86.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
205.209.185.47	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.185	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4

09-22-2016-15:04:09 to 09-22-2016-16:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.210.140.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	137
80.246.136.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
80.246.138.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
46.19.86.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
88.202.218.243	United Kingdom	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
46.19.86.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
46.19.85.2	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.85.2	Block	6
84.109.68.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
79.181.27.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.126.83.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.225.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.132.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.111.153.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
212.199.121.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.55.40.73	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
192.116.91.101	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$questionUpdate$hiddenUpdate Question in www.aka.idf.il/main/giyus/faq.aspx	None	1
162.247.97.162	Virgin Islands, British	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
46.19.85.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter d in www.aka.idf.il/main/giyus/general.aspx	None	1
84.94.170.66	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.151.56.41	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/foibdb7s0o4	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
46.19.85.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter c in www.aka.idf.il/main/giyus/general.aspx	None	1
108.27.235.39	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
79.183.43.37	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/undefined	Block	1
66.102.9.8	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
198.20.69.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
162.247.97.162	Virgin Islands, British	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
46.19.85.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter do in www.aka.idf.il/main/giyus/general.aspx	None	1
222.254.34.165	Vietnam	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/index.php	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
46.19.85.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ca in www.aka.idf.il/main/giyus/general.aspx	None	1
66.102.9.26	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
204.79.180.117	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
169.229.3.91	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
46.19.85.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter doc in www.aka.idf.il/main/giyus/general.aspx	None	1
2.53.4.9	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1119-he/nakhal.aspx	Block	1
46.19.86.191	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
46.19.85.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter cat in www.aka.idf.il/main/giyus/general.aspx	None	1
157.55.39.20	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
80.246.136.30	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.30	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8870-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Malformed URL	Block	1
46.19.85.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
84.229.50.111	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
77.138.132.139	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
46.120.178.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/goyus	Block	1
188.32.110.160	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
157.55.39.161	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.161	Block	1

09-22-2016-15:04:09 to 09-22-2016-16:04:09