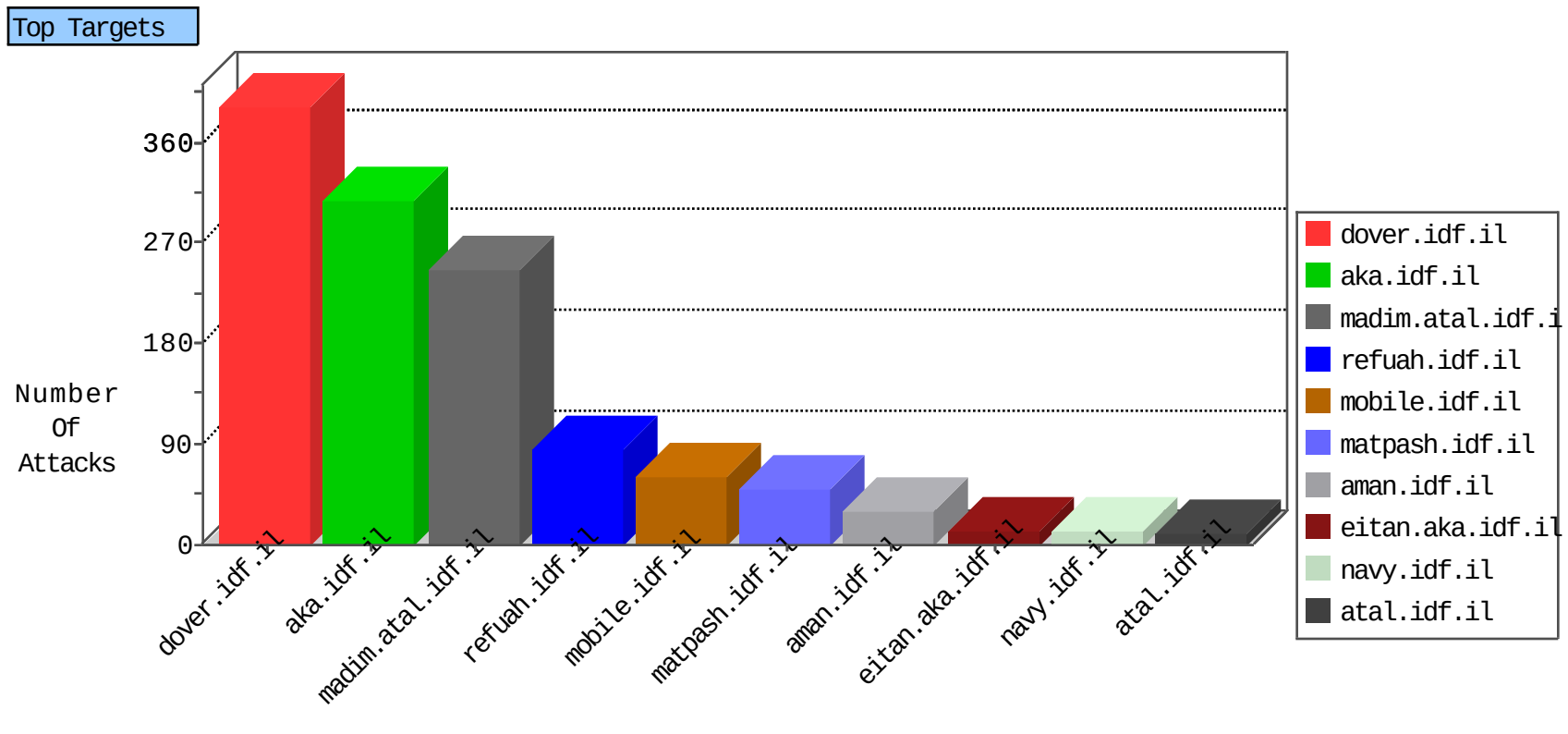
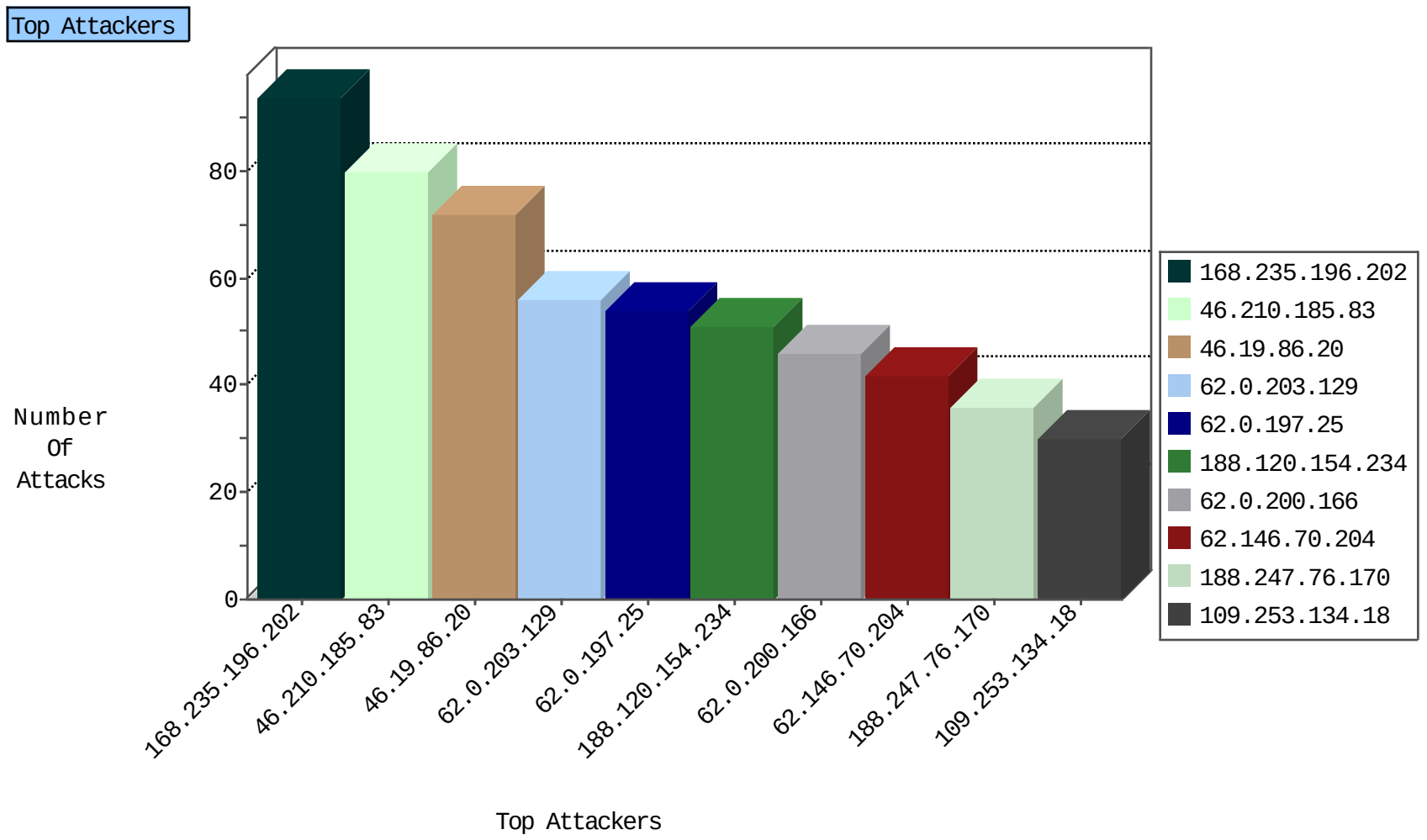
09-29-2016-08:04:07 to 09-29-2016-09:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-29-2016-08:04:07 to 09-29-2016-09:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.210.161.62	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
168.235.196.202	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
2.53.185.220	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
2.55.147.94	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
148.177.168.117	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
192.69.89.173	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1
192.69.89.173	United States	147.237.76.200	eitan.aka.idf.i	Black List	drop	1
194.90.66.15	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

09-29-2016-08:04:07 to 09-29-2016-09:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.143.245	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
199.58.86.206	United States	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-29-2016-08:04:07 to 09-29-2016-09:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.146.70.204	147.237.77.176	Germany	matpash.idf.il	Tehila - Perl LWP with fake user agent	32
79.182.30.35	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.105	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
46.172.91.21	147.237.77.74	Ukraine	law.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.218.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.136	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.76.10.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
115.28.88.243	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
5.22.134.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.128.173	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.55.19.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.131.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.137	147.237.0.34	Europe	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
46.39.53.46	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN NMAP -sS window 1024	1
212.199.121.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.63.28.189	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
132.64.187.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.203.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.153.159	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.136.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.154.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-29-2016-08:04:07 to 09-29-2016-09:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.196.202	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	90
62.0.203.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	56
62.0.200.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	46
62.0.197.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
188.247.76.170	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
62.0.200.163	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
109.253.223.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
2.53.171.79	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.0.197.25	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	12
85.64.23.138	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
46.19.86.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
62.0.200.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.136.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
87.70.7.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.55.152.166	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.116.108.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
2.53.45.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.10.252	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.124	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
212.179.218.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.179.218.166	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
5.22.134.253	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.197.51	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.26	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
65.55.210.165	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.179.218.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.134.18	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.210.161.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.134.18	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.86.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.102	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.102	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
109.253.134.18	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
157.55.2.151	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.158.25	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
81.218.203.195	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.253.134.18	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
66.249.64.163	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

09-29-2016-08:04:07 to 09-29-2016-09:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.210.185.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
46.19.86.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
188.120.154.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
37.26.146.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.13.236.80	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1390	Block	8
109.64.87.49	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	6
2.55.191.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
77.138.230.214	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	5
62.146.70.204	Germany	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	5
82.81.60.249	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 82.81.60.249	Block	5
109.253.146.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.146.70.204	Germany	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 62.146.70.204	Block	3
91.235.224.8	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/admin/cms_wysiwyg/directive/index/	Block	3
77.125.56.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.171.79	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.144.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.139.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.150.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.136.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.143.33	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	2
37.26.149.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
77.138.138.60	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
91.235.224.8	Ukraine	147.237.77.176	matpash.idf.il	Multiple Admin Blocking from 91.235.224.8	Block	2
212.199.118.19	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/titlecap.png	Block	1
82.81.60.249	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
46.19.85.177	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
180.97.106.37	China	147.237.77.235	sviva.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
180.97.106.37	China	147.237.72.156	aman.idf.il	Distributed NULL Character in Method	Block	1
176.13.17.58	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
66.249.66.202	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19666-he/idfgdover.aspx	Block	1
46.116.104.43	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
180.97.106.161	China	147.237.76.42	refuah.idf.il	Distributed NULL Character in Method	Block	1
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/images/1.he/titlecap.png	Block	1
10.161.50.81		147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	1
180.97.106.37	China	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 180.97.106.37	Block	1
180.97.106.37	China	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple NULL Character in Method from 180.97.106.37	Block	1
121.42.54.54	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
217.69.133.225	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter sidescroll in aka.idf.il/giyus/leshakot/	None	1
84.94.52.110	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
180.97.106.37	China	147.237.77.235	sviva.idf.il	Distributed NULL Character in Method	Block	1
180.97.106.37	China	147.237.76.200	eitan.aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
77.138.240.71	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8942-he/refuah.aspx	Block	1
46.117.94.79	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
180.97.106.161	China	147.237.77.233	atal.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.56.171	Block	1
180.97.106.37	China	147.237.77.216	dover.idf.il	Multiple NULL Character in Method from 180.97.106.37	Block	1

09-29-2016-08:04:07 to 09-29-2016-09:04:07