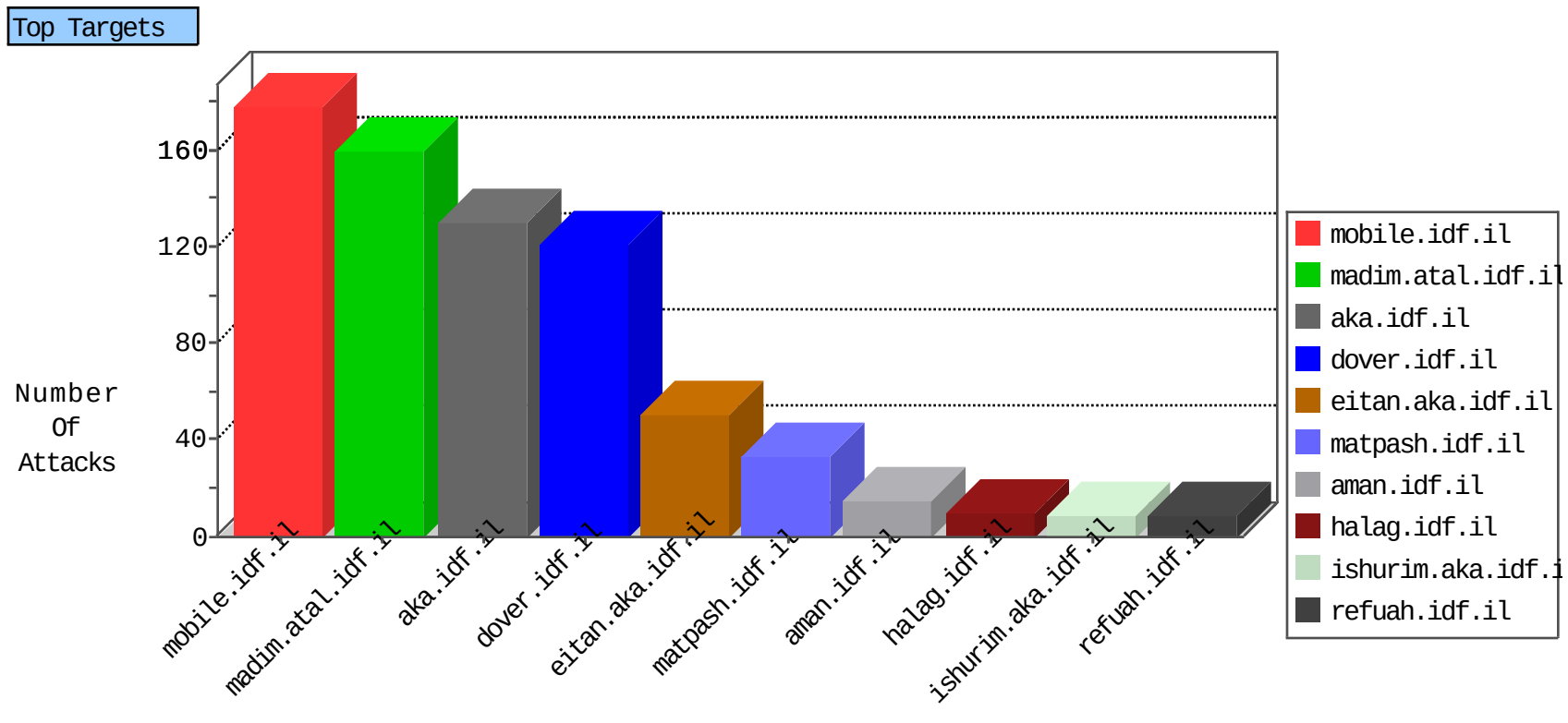
10-04-2016-22:04:01 to 10-04-2016-23:04:01

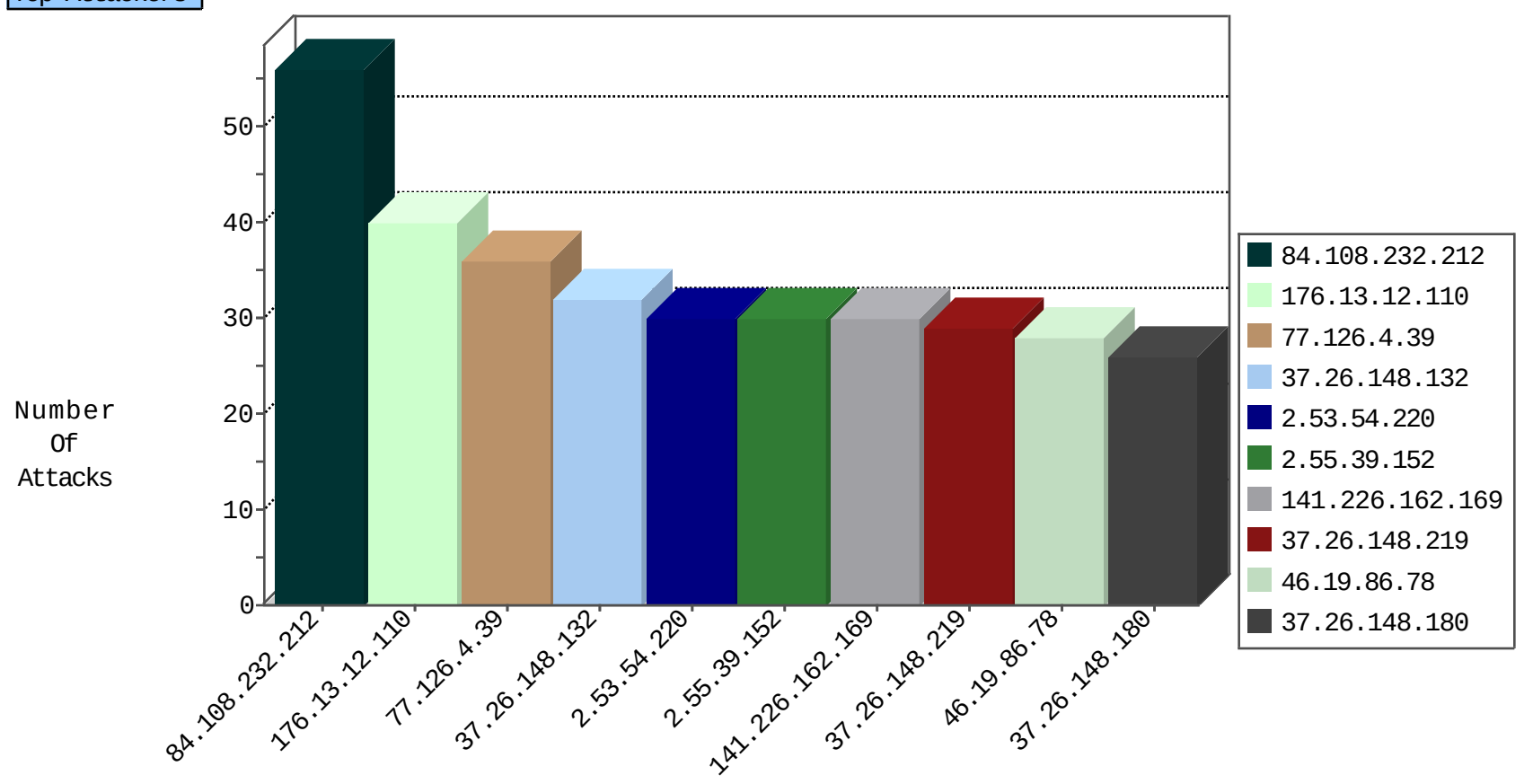
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-04-2016-22:04:01 to 10-04-2016-23:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.62.53.168	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	2
185.94.111.1	Russian Federation	147.237.76.44	e.refuah.idf.il	Black List	drop	1
71.6.216.36	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1
89.248.172.16	Netherlands	147.237.76.196	e.sviva.idf.il	Black List	drop	1
93.174.94.235	Netherlands	147.237.76.200	eitan.aka.idf.il	Black List	drop	1

10-04-2016-22:04:01 to 10-04-2016-23:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.154.189.204	Russian Federation	147.237.77.216	dover.idf.il	1090: HTTP: IIS .asp Source Code Read	Permit	2
37.9.122.201	Russian Federation	147.237.77.216	dover.idf.il	1090: HTTP: IIS .asp Source Code Read	Permit	2
89.98.142.25	Netherlands	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
178.154.189.201	Russian Federation	147.237.77.216	dover.idf.il	1090: HTTP: IIS .asp Source Code Read	Permit	2
178.154.189.202	Russian Federation	147.237.77.216	dover.idf.il	1090: HTTP: IIS .asp Source Code Read	Permit	2

10-04-2016-22:04:01 to 10-04-2016-23:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
117.21.248.87	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	147.237.77.243	Turkey	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
66.240.213.93	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
209.126.230.71	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
183.129.160.229	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
46.229.223.8	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
117.21.248.87	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.210	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
84.109.147.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.240.213.93	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
217.23.6.58	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
50.245.143.138	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
183.129.160.229	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
46.117.113.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
117.21.248.87	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1

10-04-2016-22:04:01 to 10-04-2016-23:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.126.4.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.53.54.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.55.39.152	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
141.226.162.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.13.12.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
134.134.139.76	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.78	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.53.28.113	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.12.110	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
109.65.105.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
85.65.186.245	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
80.246.140.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.12.110	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
2.122.243.211	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
2.53.169.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.26.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.130.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.55.148.12	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.158	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.55.148.12	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.208.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.78	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.78	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
181.92.98.158	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
93.86.75.231		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.180.220.108	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
93.212.141.177	Germany	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
89.139.116.35	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.88.99.146	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.246.139.199	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.129.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.12.110	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.65.55.126	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
37.26.147.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.121.235.90	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
185.3.147.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.109.116.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
185.3.147.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.151.45	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
5.102.241.211	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
61.216.2.15	Taiwan	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
141.226.218.22	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.177.159.45	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
5.22.134.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.232.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
37.26.148.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
37.26.148.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
37.26.148.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
37.26.148.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.28.113	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.166.240.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.45.87	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.45.87	Block	2
80.246.140.58	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.93	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
80.246.140.219	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
178.154.189.201	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/english/main.asp.	Block	1
2.53.26.54	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
201.175.132.121	Mexico	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
61.216.2.15	Taiwan	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
37.26.148.145	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catI in www.aka.idf.il/main/giyus/general.aspx	None	1
109.253.130.43	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.139.199	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
24.158.118.76	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Name	Block	1
66.249.66.234	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/1/1381.pdf	Block	1
178.154.189.202	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/english/main.asp.	Block	1
87.69.79.97	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
77.139.111.145	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	1
207.46.13.58	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm&	Block	1
24.158.118.76	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method ,[[#0]][[#0]][[#0]][[#19]]ñ[ÉÙÏ`¿ª•¾ŸHfÔ6[[#16]][[#7]]•¹,ÃÂ×õSS,6 À[[#30]]©'[[#25]]ª±VcK¼ü•Ë[[#16]]-½-$Lur8ù²!ÒÜƒ:[[#1]]Ä%•[[#12]]ç[[#28]]Ðqëð•[[#29]]"•Êýú[[#2]]Ü[[#25]]	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
178.154.189.204	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp.	Block	1
37.26.148.145	Israel	147.237.72.166	aka.idf.il	Unknown Parameter c in www.aka.idf.il/main/giyus/general.aspx	None	1
91.78.222.207	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
2.53.169.92	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.179.107.249	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
66.249.64.30	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8766-he/refuah.aspx	Block	1
143.202.57.50	Brazil	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/videos	Block	1
24.158.118.76	United States	147.237.76.86	navy.idf.il	Illegal HTTP Version	Block	1
68.180.229.178	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
185.120.125.67	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.117.4.111	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.148.145	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ca in www.aka.idf.il/main/giyus/general.aspx	None	1
93.212.141.177	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
5.102.195.97	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
79.182.132.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.15	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
157.55.39.92	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/chinuch/miktzoa/default.asp	None	1
24.158.118.76	United States	147.237.76.86	navy.idf.il	NULL Character in Method ,[[#0]][[#0]][[#0]][[#19]]ñ[ÉÙÏ`¿ª•¾ŸHfÔ6[[#16]][[#7]]•¹,ÃÂ×õSS,6 À[[#30]]©'[[#25]]ª±VcK¼ü•Ë[[#16]]-½-$Lur8ù²!ÒÜƒ:[[#1]]Ä%•[[#12]]ç[[#28]]Ðqëð•[[#29]]"•Êýú[[#2]]Ü[[#25]]	Block	1
77.138.26.183	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/faq.aspx	Block	1