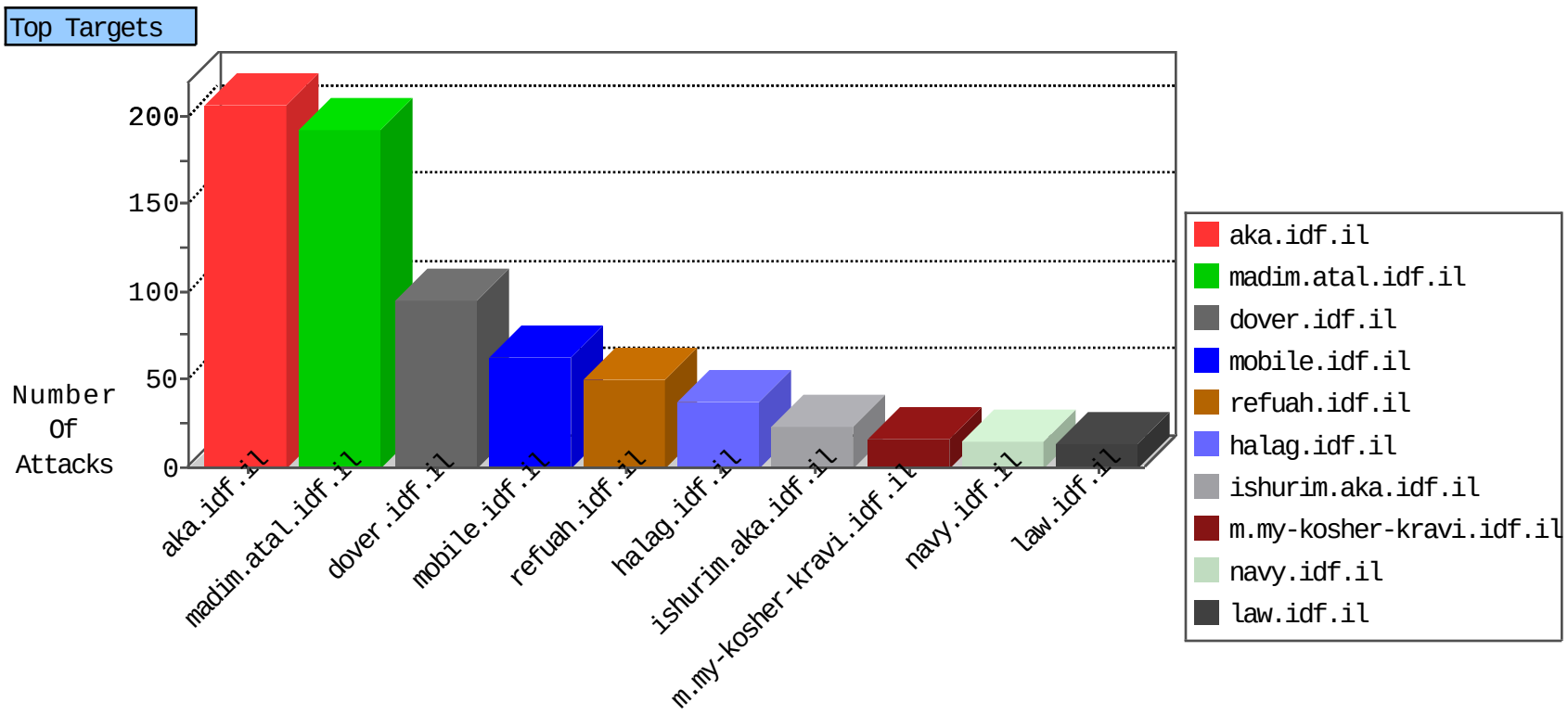
09-21-2016-08:04:01 to 09-21-2016-09:04:01

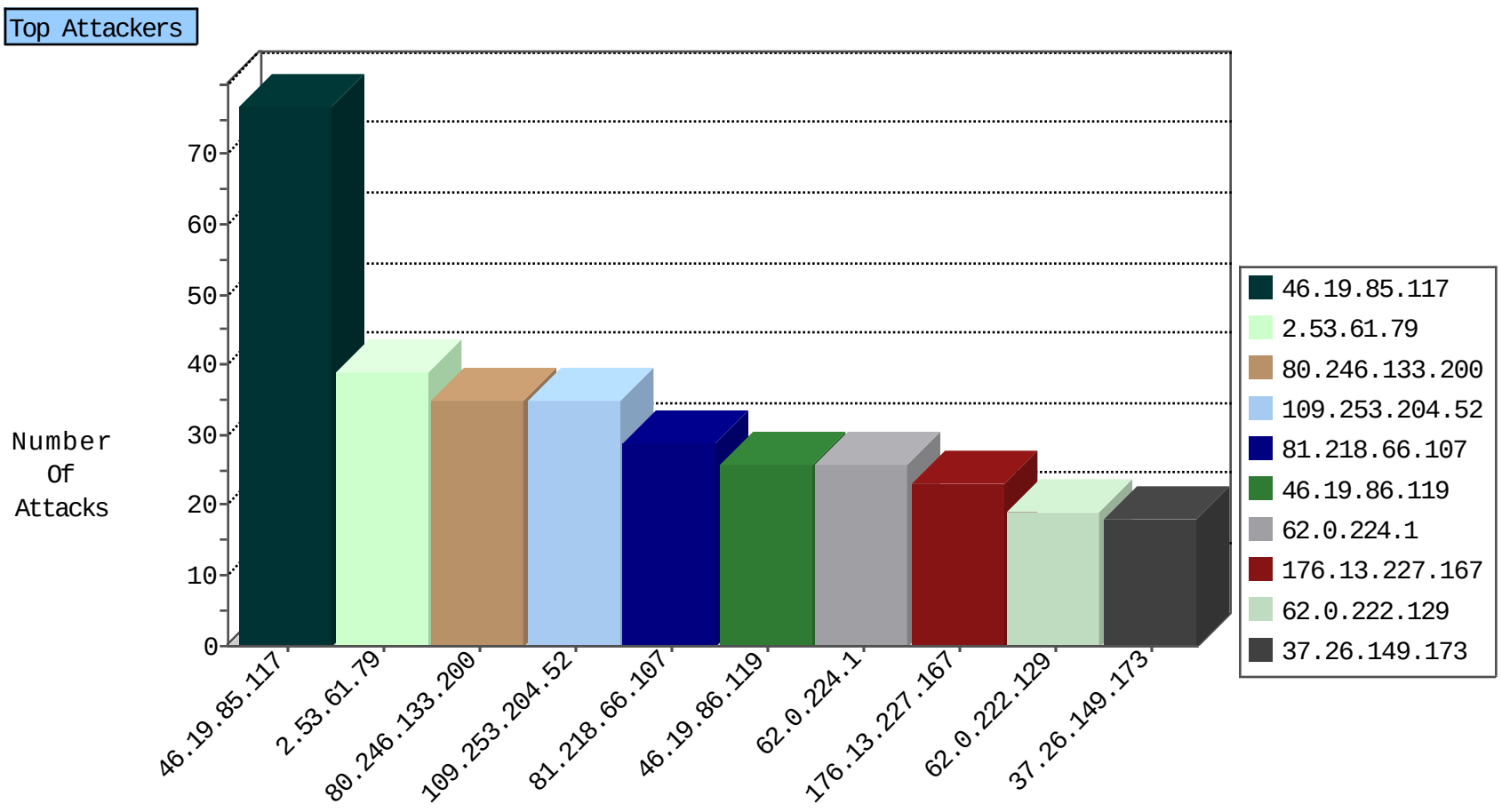
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-21-2016-08:04:01 to 09-21-2016-09:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.66.107	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
142.54.174.82	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
173.208.197.202	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
69.30.193.254	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
185.94.111.1	Russian Federation	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
142.54.174.86	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
63.141.242.195	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
173.208.197.203	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
45.32.201.7	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.202	e.halag.idf.il	Black List	drop	1
173.208.150.115	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	1
63.141.242.198	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
173.208.197.203	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
82.221.105.6	Iceland	147.237.76.30	himush.idf.il	Black List	drop	1
52.28.32.164	Germany	147.237.76.196	e.sviva.idf.il	JLM_Purple_Con_Limit_Https	drop	1
198.204.224.234	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
173.208.150.118	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
69.30.193.250	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
185.94.111.1	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
63.141.242.195	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
204.12.220.85	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1

09-21-2016-08:04:01 to 09-21-2016-09:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.163	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

09-21-2016-08:04:01 to 09-21-2016-09:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
122.116.129.169	147.237.0.35	Taiwan	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
5.102.195.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
128.232.110.28	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
2.53.146.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
125.213.243.10	147.237.77.61	Thailand	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
104.167.6.84	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.201.80	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.130.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.7.216.31	147.237.76.196	Brazil	e.sviva.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
62.219.255.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.228.216.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.143.82.50	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
164.52.227.101	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.138.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
128.232.110.28	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN Potential SSH Scan	1
2.55.6.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
128.232.110.28	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
125.65.82.44	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
118.103.126.194	147.237.76.200	Japan	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.231.57	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
86.122.137.11	147.237.8.14	Romania	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
206.246.150.226	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.66.18	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
193.47.165.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
164.52.227.101	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.76.39	United Kingdom	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1

09-21-2016-08:04:01 to 09-21-2016-09:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.133.200	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
62.0.224.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
62.0.222.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	19
81.218.66.107	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
2.55.130.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.253.204.52	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.55.185.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.119	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	11
5.28.160.203	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.0.21	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.253.216.218	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
83.130.242.97	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.206	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
195.200.205.2	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
46.19.86.206	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.111.244.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.31.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
109.253.203.202	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
84.111.61.12	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.21	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.157.210	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
105.201.251.147	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.28.160.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.86.242	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
81.218.40.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
46.19.86.27	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
105.201.251.147	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
81.218.40.194	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
84.111.21.92	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
213.8.71.26	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.4	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.246.137.34	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	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
93.184.15.247	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
84.108.130.182	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	3
37.26.148.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.111.78.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.108.130.182	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.149.229	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.4	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.111.157.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.147.172	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	2
105.201.251.147	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2

09-21-2016-08:04:01 to 09-21-2016-09:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
2.53.61.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
176.13.227.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
109.253.204.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
37.26.149.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.86.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.144.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.174.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.32.62	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
109.253.198.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	2
46.19.85.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.148.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-22724-he/idfgdover.aspx	Block	1
200.135.184.250	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	NULL Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]'¢TR‰€ZÐ[[#12]]}üû›Í9v¼ÈõZ¸}Þºvø={ï•‹[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À	Block	1
2.55.155.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
199.203.251.216	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
80.246.133.200	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.64.181	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
213.8.71.26	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	1
200.135.184.250	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal HTTP Version	Block	1
68.180.230.183	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
46.19.86.139	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
200.135.184.250	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/changelog.txt	Block	1
2.55.187.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
200.135.184.250	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	Abnormally Long Request method	Block	1
82.80.133.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.94	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/894-he	Block	1
200.135.184.250	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	Malformed HTTP Header Line 2	Block	1
79.177.227.23	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
46.116.64.63	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
200.135.184.250	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]'¢TR‰€ZÐ[[#12]]}üû›Í9v¼ÈõZ¸}Þºvø={ï•‹[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À in URL ¸[[#20]]¸	Block	1
200.135.184.250	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Header Name [[#0]]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
213.151.35.212	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21685-he/idfgdover.aspx	Block	1
200.135.184.250	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	Malformed URL ¸[[#20]]¸	Block	1
46.19.85.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
132.74.95.19	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/109151.pdf	Block	1
79.179.188.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.219.160.157	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
204.79.180.162	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
200.135.184.250	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]'¢TR‰€ZÐ[[#12]]}üû›Í9v¼ÈõZ¸}Þºvø={ï•‹[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À	Block	1
100.38.228.127	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
217.194.202.180	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.75.173	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding aI_;fAQ&e>{GbP6@ywx@zx!d/u58^O/QN){GDx1akZ.v{MDZ42FdE_vwL-@_o)3ii;1 in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
200.135.184.250	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	NULL Character in Header Name at [[#1]][[#0]][[#0]]6[[#0]][[#5]][[#0]][[#5]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]][[0]]	Block	1
80.230.227.158	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1

09-21-2016-08:04:01 to 09-21-2016-09:04:01