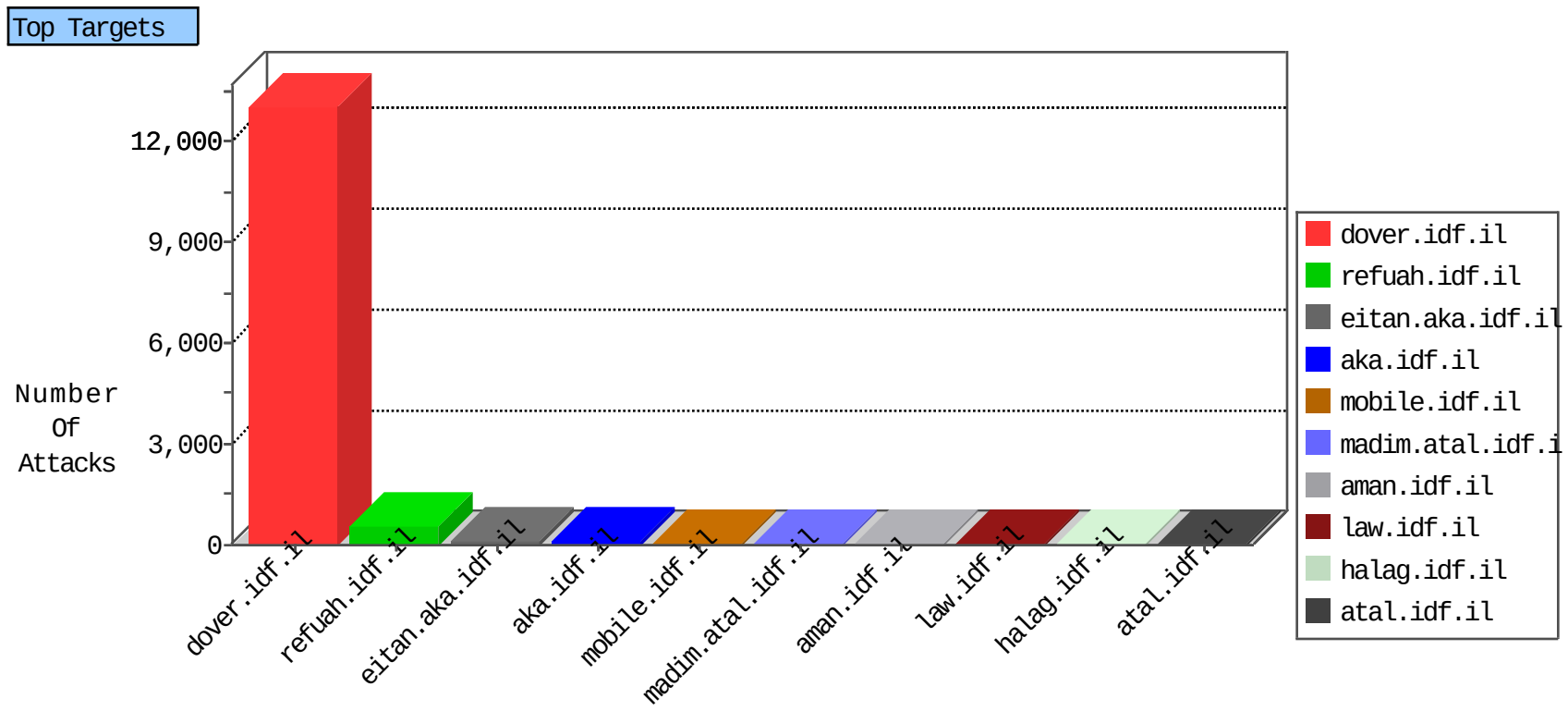
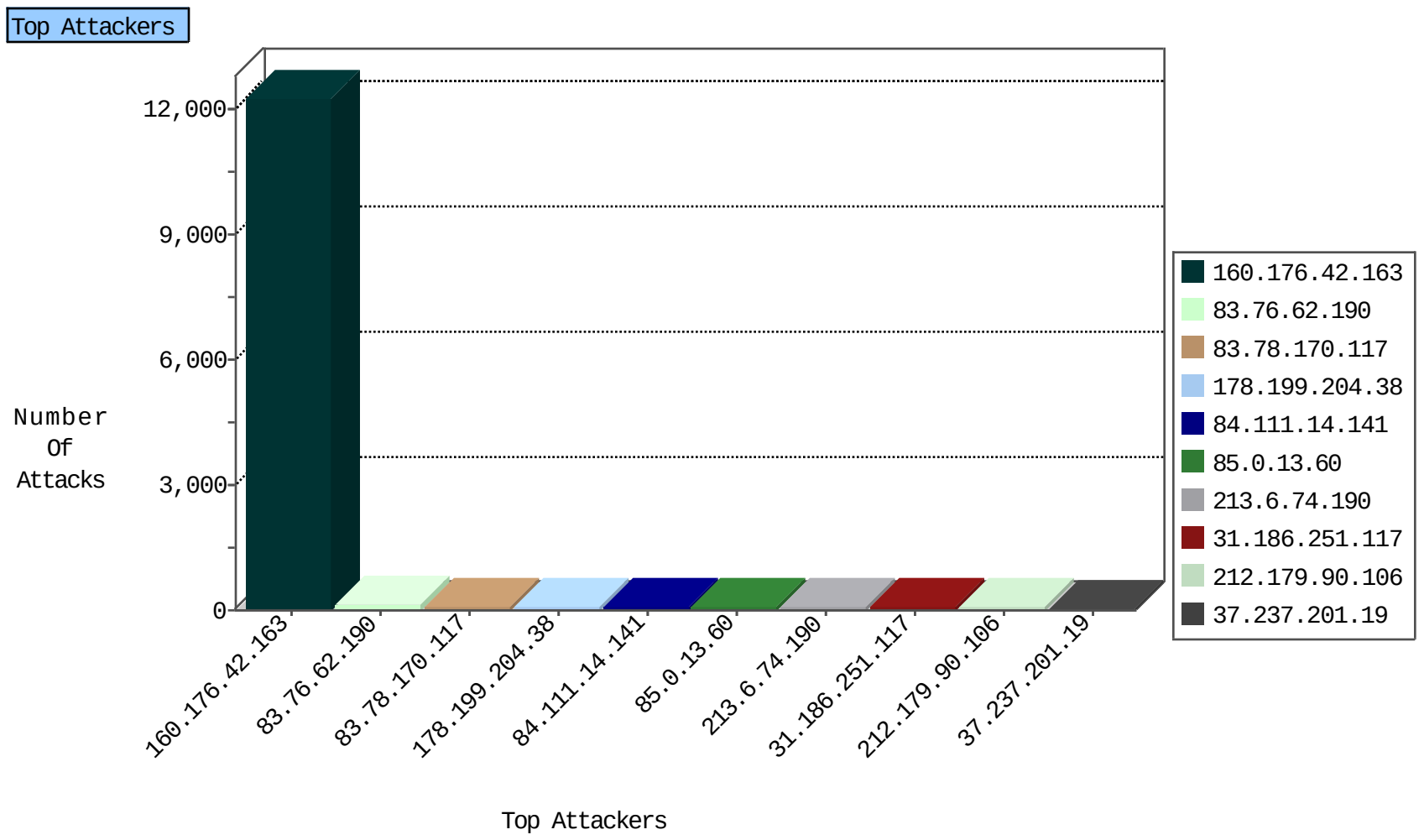
10-02-2016-15:04:08 to 10-02-2016-16:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-02-2016-15:04:08 to 10-02-2016-16:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	dest-reset	245
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	30
134.147.203.115	Germany	147.237.76.39	mobile.meitav.idf.il	Black List	drop	2
93.174.94.235	Netherlands	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
173.208.198.10	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	1
173.208.213.195	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
173.208.213.196	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1

10-02-2016-15:04:08 to 10-02-2016-16:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
71.6.146.185	United States	147.237.76.39	mobile.meitav.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

10-02-2016-15:04:08 to 10-02-2016-16:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	3
171.247.244.142	147.237.77.216	Vietnam	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
94.102.48.194	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.243.100	147.237.77.61	France	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.91.21	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.59.11	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
14.45.247.84	147.237.72.167	Korea, Republic of	ishurim.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
208.100.26.228	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
185.120.124.35	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
94.102.48.194	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.8.46	Turkey	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.91.21	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.48	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
14.126.82.5	147.237.77.19	China	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.255.90.133	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.9.129.14	147.237.8.27	Russian Federation	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.194	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1

10-02-2016-15:04:08 to 10-02-2016-16:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9643
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	987
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	667
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	399
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	225
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	123
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	87
84.111.14.141	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
213.6.74.190	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	drop		drop	68
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
37.237.201.19	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
31.222.233.211	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
79.180.201.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
176.13.230.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
83.78.170.117	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	23
83.76.62.190	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
83.78.170.117	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
83.76.62.190	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	22
31.186.251.117	Germany	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	22
83.76.62.190	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	22
178.199.204.38	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	21
83.76.62.190	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	21
83.78.170.117	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	21
178.199.204.38	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
83.78.170.117	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	21
83.76.62.190	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
178.199.204.38	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	20
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
85.0.13.60	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
178.199.204.38	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	20
178.199.204.38	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
85.0.13.60	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	19
31.186.251.117	Germany	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	19
85.0.13.60	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	18
85.0.13.60	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	18
85.0.13.60	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
31.186.251.117	Germany	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	18
83.78.170.117	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
94.142.34.211	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
185.27.105.140	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
109.253.221.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
37.26.147.217	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
2.55.174.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.181.96.88	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
78.27.148.187	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
185.120.124.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.53.134.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10

10-02-2016-15:04:08 to 10-02-2016-16:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.132.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
185.32.179.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.132.212	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	4
176.13.229.64	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
109.64.187.82	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
185.120.124.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.73.158	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/ain/giyus	Block	3
77.138.65.41	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	3
95.35.148.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
141.226.147.210	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
213.8.204.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.14.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	Unauthorized Method POST for 147.237.77.216/	Block	1
98.218.140.83	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/yohalan	Block	1
5.102.253.49	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	1
79.180.255.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in URL	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Malformed URL -#012£[[#25]]:[[<ת#24[[]]#18n]]Ÿ¸%³:[[0#]]Ð»	Block	1
66.249.65.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
139.162.13.205	Singapore	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method	Block	1
5.102.253.49	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
5.22.134.99	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
94.199.151.22	United Kingdom	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.76.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/personalentrance.asp	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method ÓxG[[#16]],‡¸ïñŽ in URL	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Abnormally Long Request request version	Block	1
5.102.253.49	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name œ[[#16]]=hòkÔŠú#011µ¸€[[#18]]xæ'(&÷	Block	1
79.183.39.16	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Unknown HTTP Request Method hž¥[[#27]]—aZä<K7ÐK˜[[#17]]Ëë‡I[[#6]]6=Î4pk™Ÿ in URL	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	NULL Character in URL -#012£[[#25]]:[[<ת#24[[]]#18n]]Ÿ¸%³ »Ð]]#0[[:	Block	1
66.249.65.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/statistics/terror	Block	1
5.255.253.75	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
139.162.13.205	Singapore	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
5.102.253.49	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
77.127.74.118	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_text.asp	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Method †F•Öy¹o)•	Block	1
5.102.253.49	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Abnormally Long Request method	Block	1
79.183.68.31	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unknown HTTP Request Method †F•Öy¹o)• in URL]]Ð»0#:[[¸%³Ÿn]]81#]][[42#]]:Л<[[52#[[£210#-	Block	1
66.249.69.116	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/masaiyot26122010.aspx	Block	1
46.19.85.149	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.102.253.49	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Abnormally Long Request method	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in URL -#012£[[#25]]:Л <[[#24]][[#18]]nŸ³%¸[[:#0Ð]]»	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	1

10-02-2016-15:04:08 to 10-02-2016-16:04:08