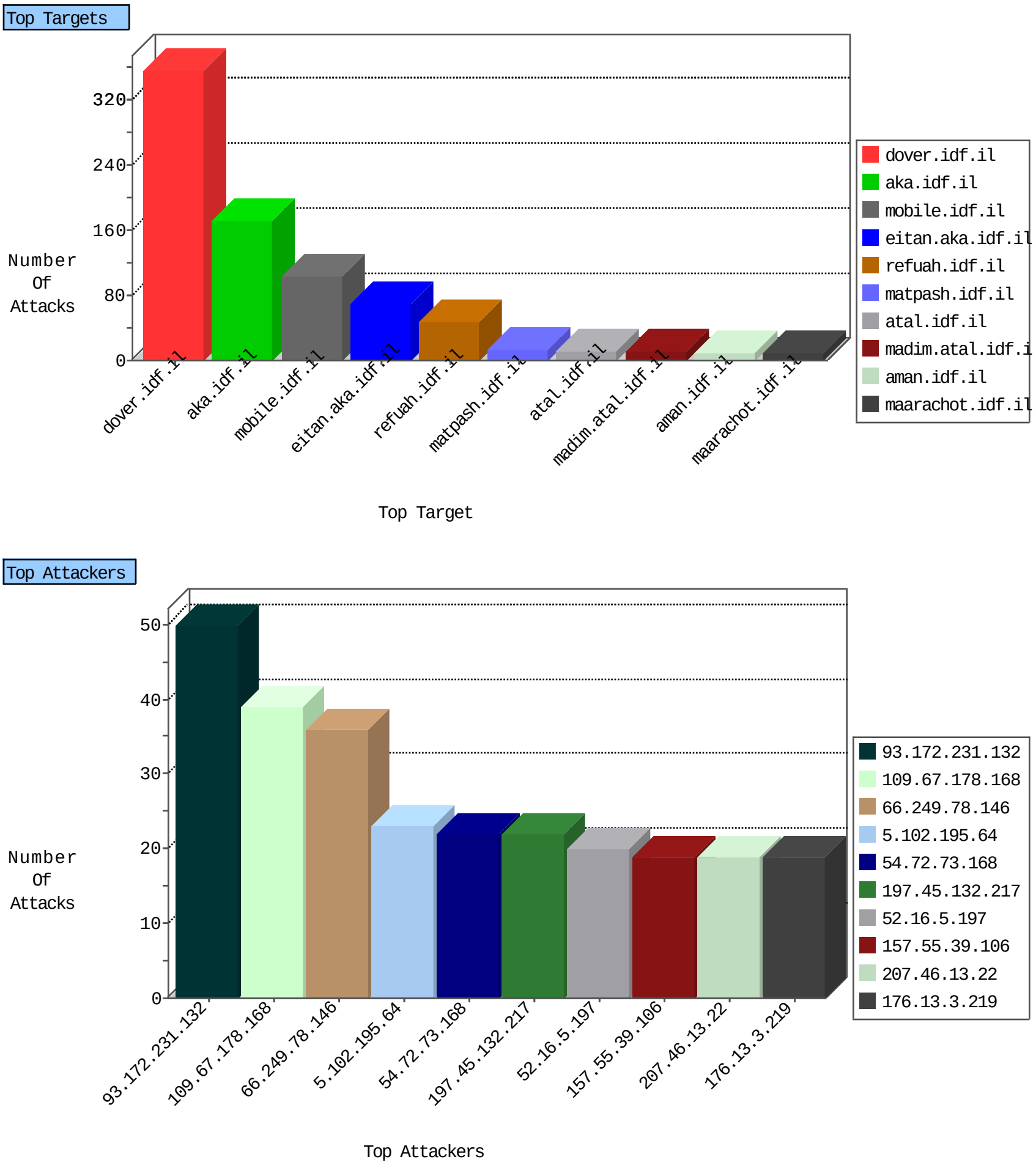
04-30-2016-18:04:04 to 04-30-2016-19:04:04

IDF Under Attack Daily Report



04-30-2016-18:04:04 to 04-30-2016-19:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5375
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	2
209.126.136.2	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-30-2016-18:04:04 to 04-30-2016-19:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-30-2016-18:04:04 to 04-30-2016-19:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
107.158.255.194	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 4096	1
106.184.2.29	147.237.76.177	Japan	ncore.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
222.255.180.117	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN Potential SSH Scan	1
210.212.93.46	147.237.72.217	India	e.idf.il	ET SCAN Potential SSH Scan	1
156.212.53.82	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 4096	1
107.158.255.194	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 3072	1
89.248.167.131	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
222.255.180.117	147.237.76.30	Vietnam	himush.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.255.180.117	147.237.0.15	Vietnam	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

04-30-2016-18:04:04 to 04-30-2016-19:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.172.231.132	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
109.67.178.168	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
5.102.195.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.19.85.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.3.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
5.9.73.227	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
86.22.242.6	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
128.242.249.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
89.128.25.196	Spain	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	8
79.177.169.247	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.176.22.83	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
79.176.22.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
87.71.82.222	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.195.64	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.6.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.151.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.27.106.28	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.46.41.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.244.123.171	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
87.71.90.125	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.102.254.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.177.169.247	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
47.17.213.93	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
8.37.232.110	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
149.78.7.37	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.116.22.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.67.98.51	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.177.169.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
87.70.72.92	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
66.249.88.88	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.114.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-30-2016-18:04:04 to 04-30-2016-19:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.102.195.64	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	5
178.137.83.178	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	4
176.13.3.219	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
185.32.179.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.68.0.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
120.76.146.29	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
84.94.75.184	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
46.19.85.87	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.53.28.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.234	Block	1
2.55.151.182	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.43	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/www.pc.co.il/	Block	1
109.67.98.51	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
80.2.143.105	United Kingdom	147.237.76.30	himush.idf.il	Malformed HTTP Header Line 1	Block	1
52.13.45.167	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1133-he/dover.aspx parameter PageNum	Block	1
120.76.146.29	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
84.109.213.156	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/mobile	Block	1
79.176.139.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.106	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
109.67.178.168	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
80.2.143.105	United Kingdom	147.237.76.30	himush.idf.il	Malformed URL	Block	1
65.55.213.27	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
120.76.146.29	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
80.2.143.105	United Kingdom	147.237.76.30	himush.idf.il	Abnormally Long Request method	Block	1
17.142.155.123	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/apple-app-site-association	Block	1
162.223.14.234	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/test/wp-admin/	Block	1
112.210.13.65	Philippines	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
80.2.143.105	United Kingdom	147.237.76.30	himush.idf.il	NULL Character in Method ¯[[#0]][[#0]][[#0]]C£[[#11]]”ÜÀa[R×P[[#27]][[#30]]¡æ¿[[#3]]•/÷ßÏd[[#7]]ô& Ñ[[#19]]•‘Zy[[#16]][[#27]]: 2[[#8]]•Ï•‰ØáÚ•m*f*–A“˜Ó˜ßæËlÓ£ÉÓªê+[[#20]]R˜W_œÂÄ[[#7]]å(É=1€„	Block	1
188.120.149.169	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
132.66.222.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
87.70.83.230	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
80.2.143.105	United Kingdom	147.237.76.30	himush.idf.il	Illegal Byte Code Character in Header Name p/žš„8•Ùæö ¨ò&Ø	Block	1
112.210.13.65	Philippines	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
80.2.143.105	United Kingdom	147.237.76.30	himush.idf.il	Unknown HTTP Request Method ¯[[#0]][[#0]][[#0]]C£[[#11]]”ÜÀa[R×P[[#27]][[#30]]¡æ¿[[#3]]•/÷ßÏd[[#7]]ô& Ñ[[#19]]•‘Zy[[#16]][[#27]]: 2[[#8]]•Ï•‰ØáÚ•m*f*–A“˜Ó˜ßæËlÓ£ÉÓªê+[[#20]]R˜W_œÂÄ[[#7]]å(É=1€„	Block	1
207.46.13.178	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
149.78.242.81	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
90.85.153.153	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
80.2.143.105	United Kingdom	147.237.76.30	himush.idf.il	Illegal Byte Code Character in Method ¯[[#0]][[#0]][[#0]]C£[[#11]]”ÜÀa[R×P[[#27]][[#30]]¡æ¿[[#3]]•/÷ßÏd[[#7]]ô& Ñ[[#19]]•‘Zy[[#16]][[#27]]: 2[[#8]]•Ï•‰ØáÚ•m*f*–A“˜Ó˜ßæËlÓ£ÉÓªê+[[#20]]R˜W_œÂÄ[[#7]]å(É=1€„	Block	1
46.19.86.246	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
176.13.7.158	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

04-30-2016-18:04:04 to 04-30-2016-19:04:04