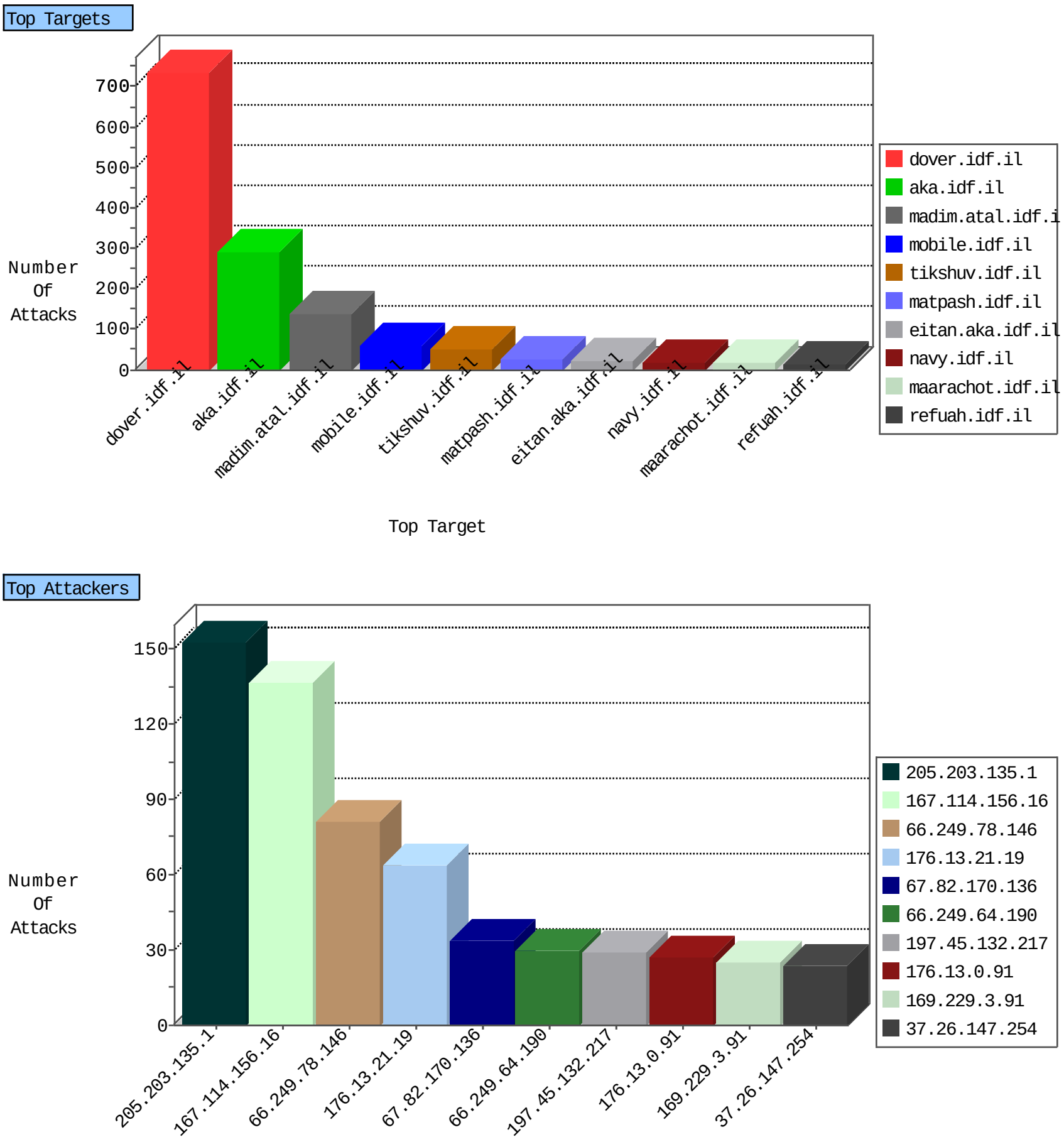
04-27-2016-11:04:04 to 04-27-2016-12:04:04

IDF Under Attack Daily Report



04-27-2016-11:04:04 to 04-27-2016-12:04:04

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	11560
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	5019
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2048
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	7
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
94.102.49.116	Netherlands	147.237.76.200	eitan.aka.idf.i	Block_Ntp_All_Net	drop	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
77.125.74.68	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1

04-27-2016-11:04:04 to 04-27-2016-12:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-27-2016-11:04:04 to 04-27-2016-12:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
24.85.73.204	147.237.76.176	Canada	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
24.85.73.204	147.237.76.86	Canada	navy.idf.il	ET SCAN Potential SSH Scan	1
212.179.61.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
24.85.73.204	147.237.76.31	Canada	nakchal.idf.il	ET SCAN Potential SSH Scan	1
162.244.10.174	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
13.82.25.17	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
106.186.113.132	147.237.76.42	Japan	refuah.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
5.29.240.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
36.72.228.72	147.237.76.42	Indonesia	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
31.220.64.37	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
24.85.73.204	147.237.76.200	Canada	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
24.85.73.204	147.237.76.148	Canada	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
24.85.73.204	147.237.76.39	Canada	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
24.85.73.204	147.237.76.30	Canada	himush.idf.il	ET SCAN Potential SSH Scan	1
122.116.97.59	147.237.0.34	Taiwan	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
13.82.25.17	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.169.126	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
36.72.228.72	147.237.76.42	Indonesia	refuah.idf.il	ET SCAN NMAP -f -sS	1
31.220.64.37	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

04-27-2016-11:04:04 to 04-27-2016-12:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	153
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
67.82.170.136	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
176.13.0.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
212.179.155.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
172.56.16.4	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
198.58.102.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.148.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.116.28.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
87.203.102.200	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
188.161.150.10	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.66.187	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
95.86.104.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
169.253.194.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.149.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.19.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.19.183	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.178.126.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.200	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
82.166.2.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.21.19	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
207.46.13.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.170.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.2.127.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.167.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.179.210.157	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
83.244.98.100	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
83.244.113.114	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
188.161.150.10	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
149.50.39.42	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

04-27-2016-11:04:04 to 04-27-2016-12:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.21.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
37.26.149.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
37.26.147.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
192.118.10.10	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	16
37.26.147.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
109.64.172.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
31.181.83.53	Russian Federation	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
91.135.102.167	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	5
31.181.83.53	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.181.83.53	Block	5
5.29.53.47	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	5
91.135.102.167	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/7/	Block	3
178.137.93.24	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 178.137.93.24	Block	3
37.26.148.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
91.135.102.167	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 91.135.102.167	Block	2
2.53.170.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
131.253.25.201	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.129.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/buttonback.png	Block	1
109.64.19.243	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.109.102.224	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
5.39.222.159	Netherlands	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Multiple NULL Character in Method from 169.229.3.91	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Illegal Byte Code Character in Method •[[#8]]ì„[[#29]]˜[[#19]]Á›Ê„Lj÷[[#17]]{[[#5]][[#31]]£¼B·MFód¥ · qòy[[#17]]Ü	Block	1
121.96.29.250	Philippines	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
46.19.85.179	Israel	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method =1%7C17; in URL __atuvs=572072d57155e7d1000	Block	1
31.181.83.53	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
178.137.93.24	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Illegal Byte Code Character in URL	Block	1
79.178.214.202	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
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in URL	Block	1
66.249.66.45	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector/	Block	1
38.111.147.84	United States	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 38.111.147.84	Block	1
207.46.13.49	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.109.102.224	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1437-he/atal.aspx	Block	1
5.153.233.130	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
176.13.19.183	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/sites-head.jpg	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Illegal Byte Code Character in URL	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/pniot.jpg	Block	1
188.161.150.10	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-he/cogat.aspx	Block	1
2.53.186.180	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	NULL Character in Method ŠXÈg9…û“[[#25]]Š&7u§7˜ânú6[[#19]]ðØì‹[[#0]][[#0]]ÈÐÞUÌ±•Ï[[#20]]‹^“[[#2]]¤Q3ñQ{-A—Ž–_}où©¼ò½Úiæ	Block	1
80.148.27.130	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.66.121	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	NULL Character in Method Åe[[#26]]s,F7v'.s¸:šåŒm÷ŒŠ_k2Z{—ç¬~'‡MË4æŠAK™ÚR[[#16]]N [[#21]]Lð¹[[#0]][[#7]]A™n…•1u[[#8]]ª½[[#24]]PÏ	Block	1
38.111.147.84	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1

04-27-2016-11:04:04 to 04-27-2016-12:04:04