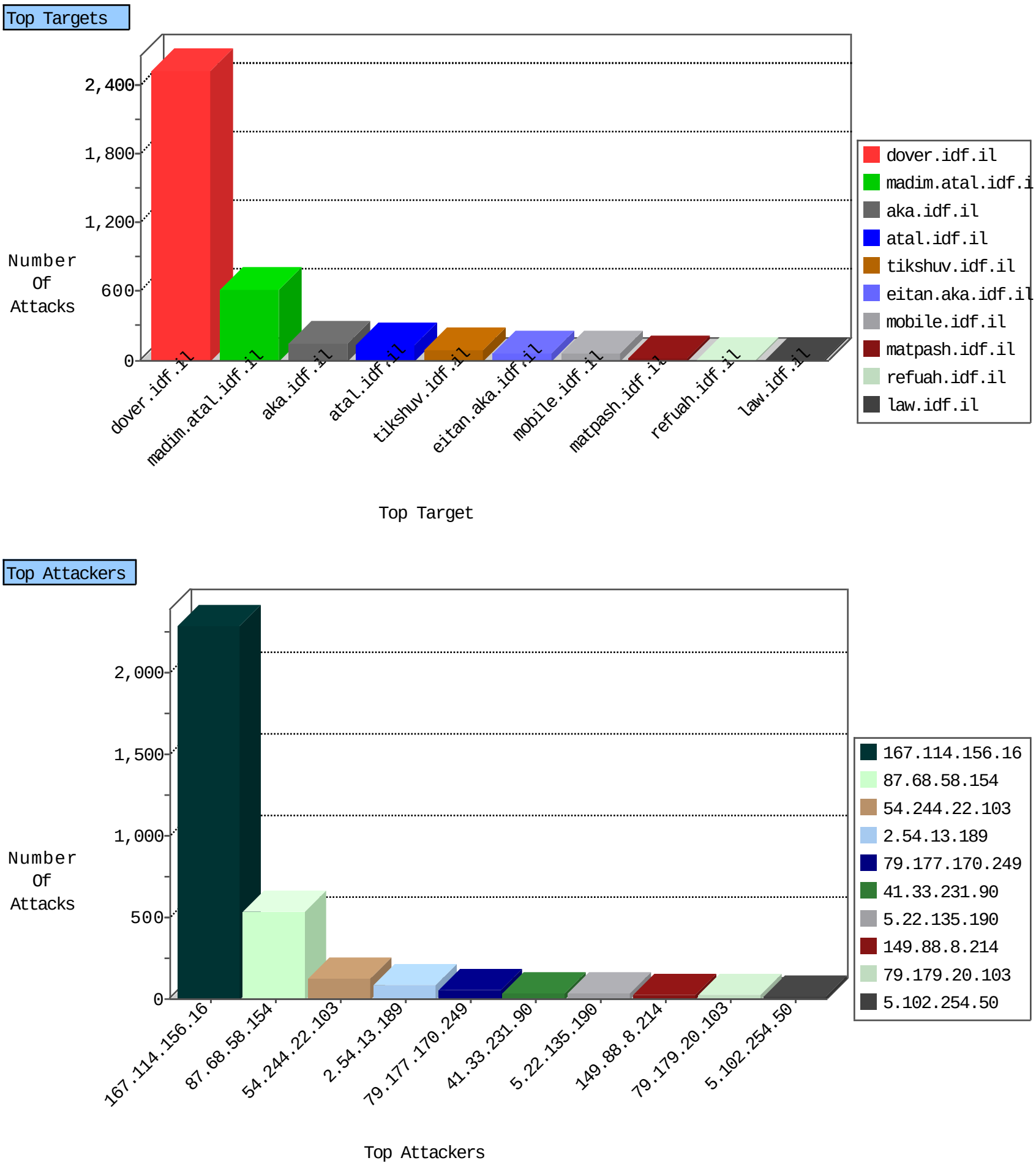
01-23-2016-11:04:01 to 01-23-2016-12:04:01

IDF Under Attack Daily Report



01-23-2016-11:04:01 to 01-23-2016-12:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.116.161.104	Israel	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	4551
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3054
46.19.86.153	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
2.54.13.189	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4
151.0.151.137	Romania	147.237.0.16	my-kosher-kravi.idf.il	L4 Source or Dest Port Zero	drop	4
87.68.148.57	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
71.6.135.131	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets_Con_Limit	drop	2
66.240.236.119	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
89.248.174.4	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
62.219.134.70	Israel	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
62.219.134.70	Israel	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
62.219.134.70	Israel	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

01-23-2016-11:04:01 to 01-23-2016-12:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.87.111	Germany	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
188.165.15.19	France	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1

01-23-2016-11:04:01 to 01-23-2016-12:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.i	Tehila - Perl LWP with fake user agent	4
163.172.13.173	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.133	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
94.102.48.195	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1

01-23-2016-11:04:01 to 01-23-2016-12:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	69
2.54.13.189	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	65
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	60
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
5.22.135.190	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
149.88.8.214	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
66.249.81.196	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.13.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
5.102.254.50	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
2.54.7.114	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.182.152.157	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.130.244	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.177.133.127	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
176.13.9.157	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
109.253.130.244	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
109.65.34.61	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.54.162.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
222.161.54.135	China	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
109.65.207.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.11.70	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.172.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.169	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.186.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.108.15.239	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.102.254.50	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.94.123.195	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
157.55.39.114	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.8.204.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.223.182.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
81.218.171.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.179.39.208	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.6.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.168	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.125.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.81	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.68.45.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.15.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.173.252.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.137.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.85.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.120.5.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.66.182	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2

01-23-2016-11:04:01 to 01-23-2016-12:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.68.58.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	305
87.68.58.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	132
87.68.58.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	103
79.177.170.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
109.160.165.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
93.173.227.254	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
109.253.213.130	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
213.57.246.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.180.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.127.184.11	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
80.246.136.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.137.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
79.179.20.103	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	2
79.176.213.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.130.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.4.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.179.20.103	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
79.179.20.103	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.78.199	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
109.66.136.100	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1247-he/atal.aspx	Block	1
79.179.20.103	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at Â±Ã"Ã¯ÂƒQÃ…Ã±BÂ?!Â£Â¿Ã„Â„ 'ÃºÂ´Â…rGtWh][[#6]]Ã¢Ã›Ã'[[#12]]Ã¢Â¯Â?tPÂ‹Â–DÂˆÂ«_Â¦Ã¢lÂ‡ [[#7]][[#25]]Â»Ã'MÃ™6Ã¯Â›[[#28]][[#0]]QÃªÂ?Âº Ã?Ã´Â™pÃ Â•Ã·Ã±t[[#21]]Â„Â¯Â‰Â›Â'1Ã¸ Â–Ã?Â«Ã?4jÃŸBÃ™Â„Ã?<ÂˆÃ =Â‰ÃŒ@Ã€Ã€~1Â„C;ÂŽ[[#8]]HÃ‰	Block	1
213.8.204.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.186	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/giyus/general.aspx	Block	1
79.179.20.103	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 2	Block	1
176.13.9.157	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
79.178.125.94	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in Header Name from 169.229.3.91	Block	1
46.19.85.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.205.82.170	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/'	Block	1
222.161.54.135	China	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/../shared/usercontrols/headerupper/	Block	1
109.92.229.83		147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
79.180.164.247	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.179.20.103	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 79.179.20.103	Block	1
196.22.142.202	South Africa	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/chamatz/klali/default.asp	None	1
109.64.172.115	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.120.68.255	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
84.228.150.235	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.179.20.103	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name Â±Ã"Ã¯ÂƒQÃ… Ã±BÂ?!Â£Â¿Ã„Â„'ÃºÂ´Â…rGtWh][[#6]]Ã¢Ã›Ã'[[#12]]Ã¢Â¯Â?tPÂ‹Â–DÂˆÂ«_Â¦Ã¢lÂ‡[[#7]][[#25]]Â»Ã'MÃ™6Ã¯Â›[[#28]][[#0]]QÃªÂ?Âº Ã?Ã´Â™pÃ Â•Ã·Ã±t[[#21]]Â„Â¯Â‰Â›Â'1Ã¸ Â–Ã?Â«Ã?4jÃŸBÃ™Â„Ã?<ÂˆÃ =Â‰ÃŒ@Ã€Ã€~1Â„C;ÂŽ[[#8]]HÃ‰	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
41.34.235.139	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
149.88.8.214	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1
109.67.52.48	Israel	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	1
79.179.20.103	Israel	147.237.72.166	aka.idf.il	NULL Character in Method [[#28]]5`[[#7]][[#2]]~Ã..Ã¦Â›*Âœ T[[#14]]Ã?rÃŽwÂ‡Ã‹Ã?IÃ?Â"Â·Ã§%Ãº&%G[[#25]]Ã§Â' [[#15]]Ã¢Ã®][[#12]]Â²ÂŽÂ¶ÂŽÂµYFÃ"F[[#14]]Â•Ã?0f[[#26]]Ã±ÃŒÃ¥"[[#18]]Ã£[[#0]]zz^Ã•[[#18]]Â‰Ã^Â¯[[#22]](\8VÃ³mÃ› fÃ?<Â¡Ã¹Ã…V/Â®[[#4]]-ÃœÂ´LÂ£9Ã»!Â¬Ã"Ã½Â–Ã„ vgÂ¬[[#2]]/1Â£Ã'_[[#6]]Ã¬ Ã?iÂ?YÂ¢Ã–Â¶] "Ã¡6Ã¿&:Â»ÂµÃŠ[[#29]]qÃ?Ã‹~[[#28]]Â'[[#29]]Ã–ÂœrÂƒhpÂ?Â^"oÂ‰ Ã¨ÂŸÃ¾2Ã•Ã†@/Â•Ã¡Â–Y[[#16]]vEÃ'Ã?Â›OÂ‹Ã¼XÂ†Â†1[[#4]]N:Ã¼	Block	1
176.13.11.70	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.120	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1

01-23-2016-11:04:01 to 01-23-2016-12:04:01