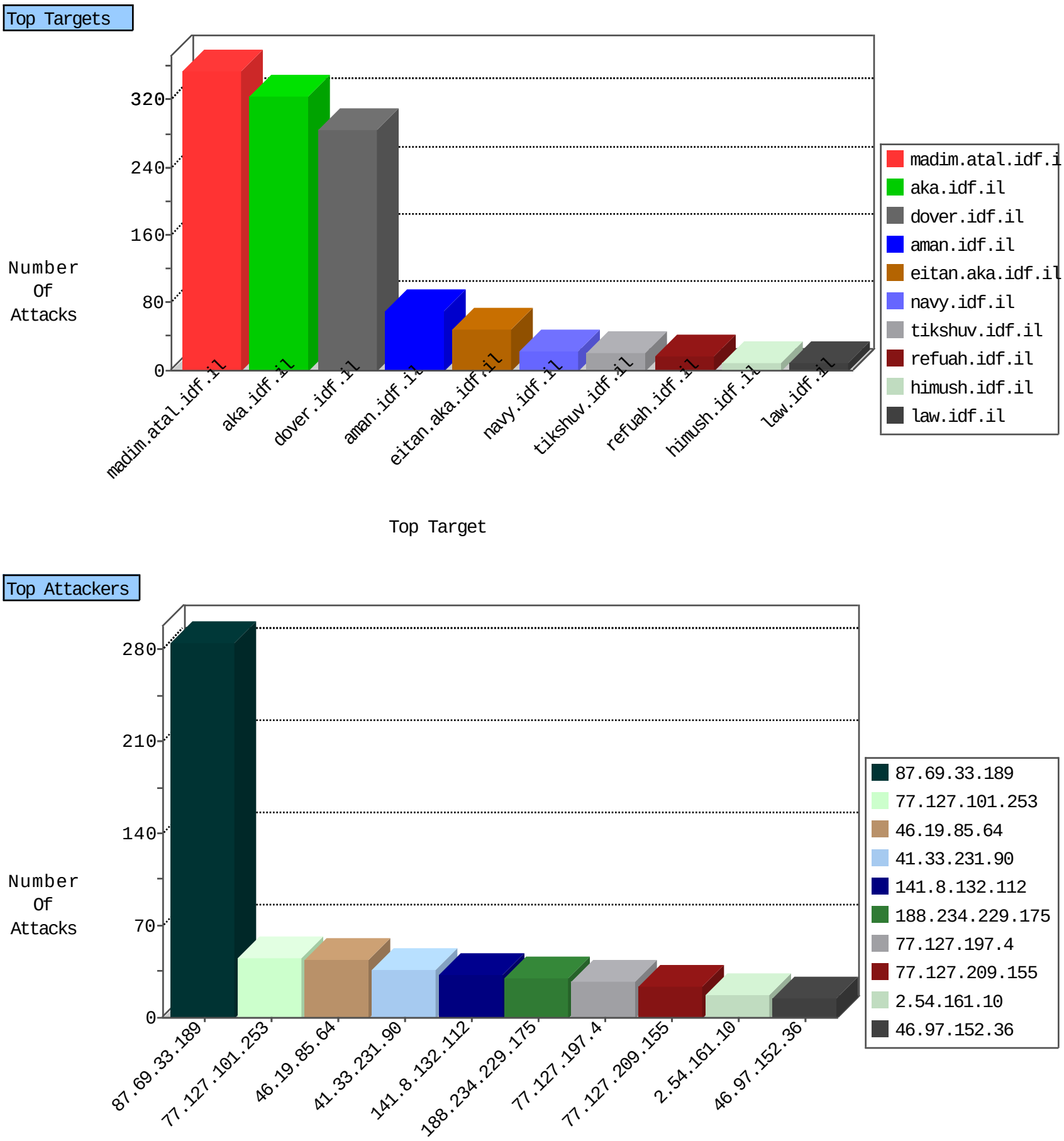
02-16-2016-22:04:04 to 02-16-2016-23:04:04

IDF Under Attack Daily Report



02-16-2016-22:04:04 to 02-16-2016-23:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.176	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	138
109.67.135.206	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
104.148.100.2	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
5.104.175.188	Bulgaria	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
173.208.206.205	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	drop	1
64.110.129.208		147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

02-16-2016-22:04:04 to 02-16-2016-23:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.90	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.196	France	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-16-2016-22:04:04 to 02-16-2016-23:04:04

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
188.234.229.175	147.237.77.216	Russian Federation	dover.idf.il	SERVER-WEBAPP backup access	3
211.215.19.235	147.237.8.46	Korea, Republic of	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
211.215.19.235	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
211.215.19.235	147.237.8.14	Korea, Republic of	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.240	147.237.72.166		aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.82.106.200	147.237.76.31	India	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
118.173.139.180	147.237.76.30	Thailand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.90.88.235	147.237.0.33	Albania	idf.il	ET SCAN Potential SSH Scan	1
211.215.19.235	147.237.8.50	Korea, Republic of	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
211.215.19.235	147.237.8.45	Korea, Republic of	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
211.215.19.235	147.237.8.24	Korea, Republic of	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.77.121	United States	e.navy.idf.il	ET DROP Dshield Block Listed Source	1
183.82.106.200	147.237.76.31	India	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
183.82.106.200	147.237.76.31	India	nakchal.idf.il	ET SCAN NMAP -f -sS	1
80.90.88.235	147.237.0.34	Albania	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

02-16-2016-22:04:04 to 02-16-2016-23:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.127.101.253	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
77.127.197.4	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	28
188.234.229.175	Russian Federation	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.97.152.36	Romania	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
50.18.94.121	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	14
79.177.133.203	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
85.130.244.74	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.81.71.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
38.106.172.130	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.182.218.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
79.178.185.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.58.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.88.92.78	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
81.218.170.8	Israel	147.237.72.166	aka.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
79.183.166.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.46.41.19	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.40.1.247	Oman	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.54.58.255	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
170.74.231.70	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.102.254.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.161.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
188.120.148.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.165.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.184	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
157.55.12.84	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.220	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.183.209.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.197.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.6.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.228.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.124.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.66.122.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
189.245.0.231	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
141.8.142.34	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.196.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.161.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
37.26.147.219	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3

02-16-2016-22:04:04 to 02-16-2016-23:04:04

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.177.63.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-16-2016-22:04:04 to 02-16-2016-23:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.33.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	174
87.69.33.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	85
46.19.85.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
87.69.33.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	15
188.120.152.152	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 188.120.152.152	Block	13
87.69.33.189	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtFirstName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	12
176.13.15.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
131.253.25.237	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
5.29.172.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.208.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.136.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.120.196.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.8.204.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.93.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/kiosk/kiosk	Block	2
5.29.92.240	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.29.92.240	Block	2
185.120.126.195		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	2
85.250.211.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
199.30.24.5	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.109.73.39	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$102 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
109.65.204.198	Israel	147.237.72.156	aman.idf.il	Malformed URL Ö¶[[#21]]oÂ¢Â¾×³â€ °[[#12]][[#18]]Â¦fÂ?×²Ö»mÂ§9[Ö¹Ö´â€"[[#7]]Ö²9sÂŽpâ€"â€ mcÖ¹[[#3]]Ã™[[#0]]~[[#26]],â€"â€™ÃŸÖ´rlÂ»oÖ²Âš×´h-â€™nl[[#20]]c×ªÃ¼bnqtÂ¸'{Â?[[#15]]2w5×¢ÃœÂ¼ÃŸ[[#7]]Â¶(ÂŸ/	Block	1
77.125.4.201	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
5.29.92.240	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$23 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
94.159.197.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.180	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/news/news.in.aspx	Block	1
46.31.103.30	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
131.253.36.205	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.228.111.97	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/ajax/updatestatus.php	Block	1
37.60.40.233	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1216-he/refuah.aspx&sa=u&ved=0ahukewjioch0lf3kahvqp5okhzkxbfwqfggjmag&usg=afqjcnhccc-ahasmmrbzxvn7r-lvl5dx_w	Block	1
109.67.9.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$23 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
207.46.13.55	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/shared/usercontrols/navmenu/	Block	1
2.54.130.70	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$116 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.65.204.198	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Value	Block	1
84.111.244.77	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
46.31.103.30	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
109.65.204.198	Israel	147.237.72.156	aman.idf.il	NULL Character in URL Ö¶[[#21]]oÂ¢Â¾×³â€ °[[#12]][[#18]]Â¦fÂ?×²Ö»mÂ§9[Ö¹Ö´â€"[[#7]]Ö²9sÂŽpâ€"â€ mcÖ¹[[#3]]Ã™[[#0]]~[[#26]],â€"â€™ÃŸÖ´rlÂ»oÖ²Âš×´h-â€™nl[[#20]]c×ªÃ¼bnqtÂ¸'{Â?[[#15]]2w5×¢ÃœÂ¼ÃŸ[[#7]]Â¶(ÂŸ/	Block	1
79.176.64.126	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$27 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.11.185.84	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.66.36	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
188.234.229.175	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.234.229.175	Block	1
46.31.103.30	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/ajax/updatestatus.php	Block	1
139.162.10.19	Netherlands	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
85.64.67.237	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
37.239.0.125	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.67.9.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$3 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
84.108.174.55	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 84.108.174.55	Block	1

02-16-2016-22:04:04 to 02-16-2016-23:04:04