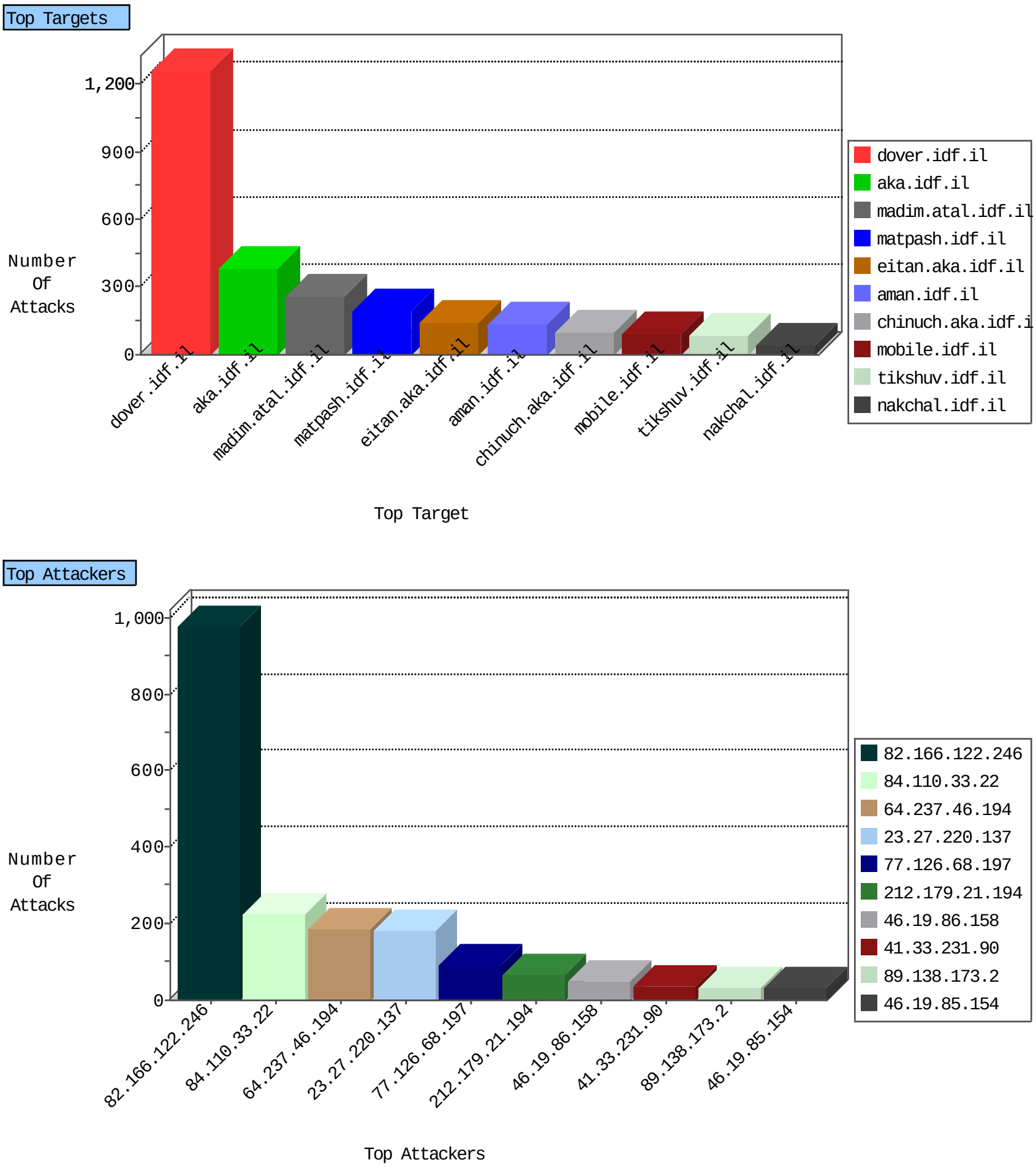
02-14-2016-17:04:04 to 02-14-2016-18:04:04

IDF Under Attack Daily Report



02-14-2016-17:04:04 to 02-14-2016-18:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.232.150	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	11
119.25.136.75	Japan	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	2
40.76.202.139	United States	147.237.72.167	ishurim.aka.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
183.11.122.177	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
178.69.38.230	Russian Federation	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
58.35.25.110	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
71.6.135.131	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1

02-14-2016-17:04:04 to 02-14-2016-18:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.98	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1

02-14-2016-17:04:04 to 02-14-2016-18:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.166.122.246	147.237.77.216	Israel	dover.idf.il	SERVER-WEBAPP WEB-INF access	18
82.166.122.246	147.237.77.216	Israel	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	4
221.139.14.120	147.237.77.216	Korea, Republic of	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.69.26	147.237.77.216	United States	dover.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
120.24.175.112	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
109.66.213.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
107.181.161.138	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.141.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.189.68	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.112	147.237.77.74	Israel	law.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
212.235.8.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.138.70.153	147.237.76.200	Sweden	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
79.138.70.153	147.237.76.44	Sweden	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
176.228.71.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
69.197.145.242	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
115.236.75.201	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
40.76.202.139	147.237.72.166	United States	aka.idf.il	ET SCAN Potential SSH Scan	1
109.65.159.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.130.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.139.189.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.7.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.242.104	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.179.122.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.77.234	United States	halag.idf.il	ET DROP Dshield Block Listed Source	1
79.138.70.153	147.237.76.177	Sweden	ncore.idf.il	ET SCAN Potential SSH Scan	1
192.114.91.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.138.70.153	147.237.0.19	Sweden	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

02-14-2016-17:04:04 to 02-14-2016-18:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	188
23.27.220.137	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	180
64.237.46.194	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	94
64.237.46.194	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	94
77.126.68.197	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
89.138.173.2	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
46.19.86.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
46.19.85.154	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.116.110.159	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
188.161.50.110	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.253.135.138	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.19.86.254	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
79.178.68.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.49.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.11.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.121.82.102	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
82.166.122.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.253.132.218	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
5.117.31.146	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.66.31.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.254	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.108.119.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.181.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.207.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.139.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.32.179.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.135.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.203	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.150.177.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.2.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
149.78.72.178	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
209.88.183.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.41.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.117.154.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
109.65.41.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
188.120.154.127	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.172	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.65.41.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.120.92.244	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

02-14-2016-17:04:04 to 02-14-2016-18:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 82.166.122.246	Block	672
84.110.33.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	113
84.110.33.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
212.179.21.194	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	67
2.54.7.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
79.177.58.171	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.177.58.171	Block	15
84.110.33.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	9
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 195.160.242.40	Block	8
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	6
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	6
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	6
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	6
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	6
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	6
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	6
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	5
46.19.85.154	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
221.139.14.120	Korea, Republic of	147.237.77.216	dover.idf.il	PHP Attempt	Block	4
176.13.11.107	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.120.199.81	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.199.81	Block	3
176.13.12.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
221.139.14.120	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 221.139.14.120	Block	3
46.19.86.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.179.154	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$3 5 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
109.253.192.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
90.209.234.3	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	2
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1806-he/dover.aspx	Block	2
46.19.85.103	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.186.189.143	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1815-he/dover.aspx	Block	2
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.12.76	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
213.57.47.94	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
87.69.32.28	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$3 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucNewsFlashControl$datepicker in www.idf.il/1153-he/dover.aspx	Block	1
188.120.148.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1415-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Illegal Byte Code Character in URL [[#14]]ÃšÂ°ubÖ¹[[#12]]Â·[[#23]] [[#7]]mâ€"×¡pd&l[[#5]]Â¨×"[[#20]]Â®Ö¸Ö¸*qÂ?[[#11]]t[[#29]]×'â€ ¦×±[[#23]]:ÖµÂ²â€ ×ŸrÂ§[[#4]]gh*Â¡×¢kz	Block	1
58.181.180.145	Thailand	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-en/cogat.aspx	Block	1
109.253.135.138	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1841-he/dover.aspx	Block	1
199.21.149.49	Canada	147.237.76.42	refuah.idf.il	Parameter Type Violation &l in www.refua.atal.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
46.19.85.203	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.110.38.142	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Multiple Directory Traversal - 1(+) from 82.166.122.246	Block	1
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1806-he/dover.aspx	Block	1
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1380-he/dover.aspx	Block	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.128	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1

02-14-2016-17:04:04 to 02-14-2016-18:04:04