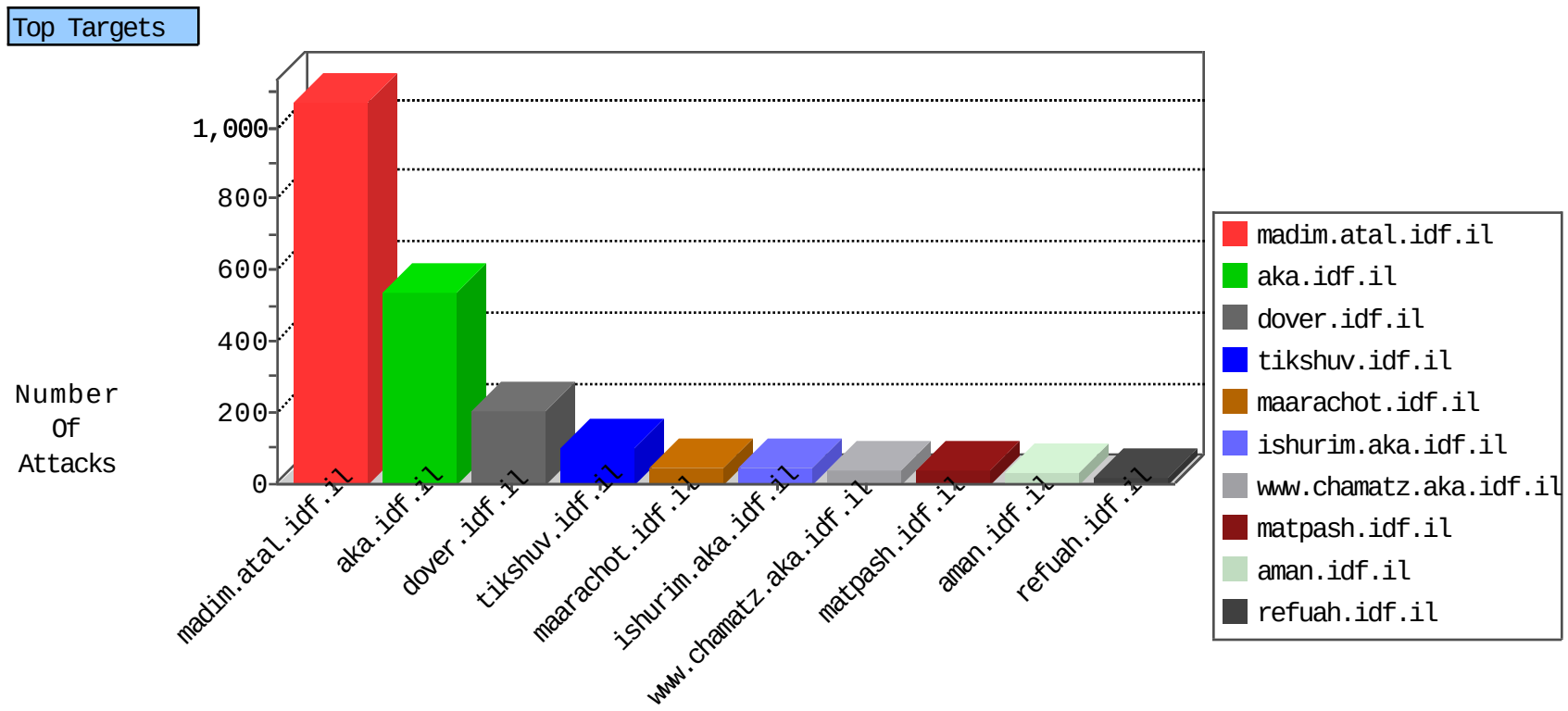
02-08-2016-16:04:09 to 02-08-2016-17:04:09

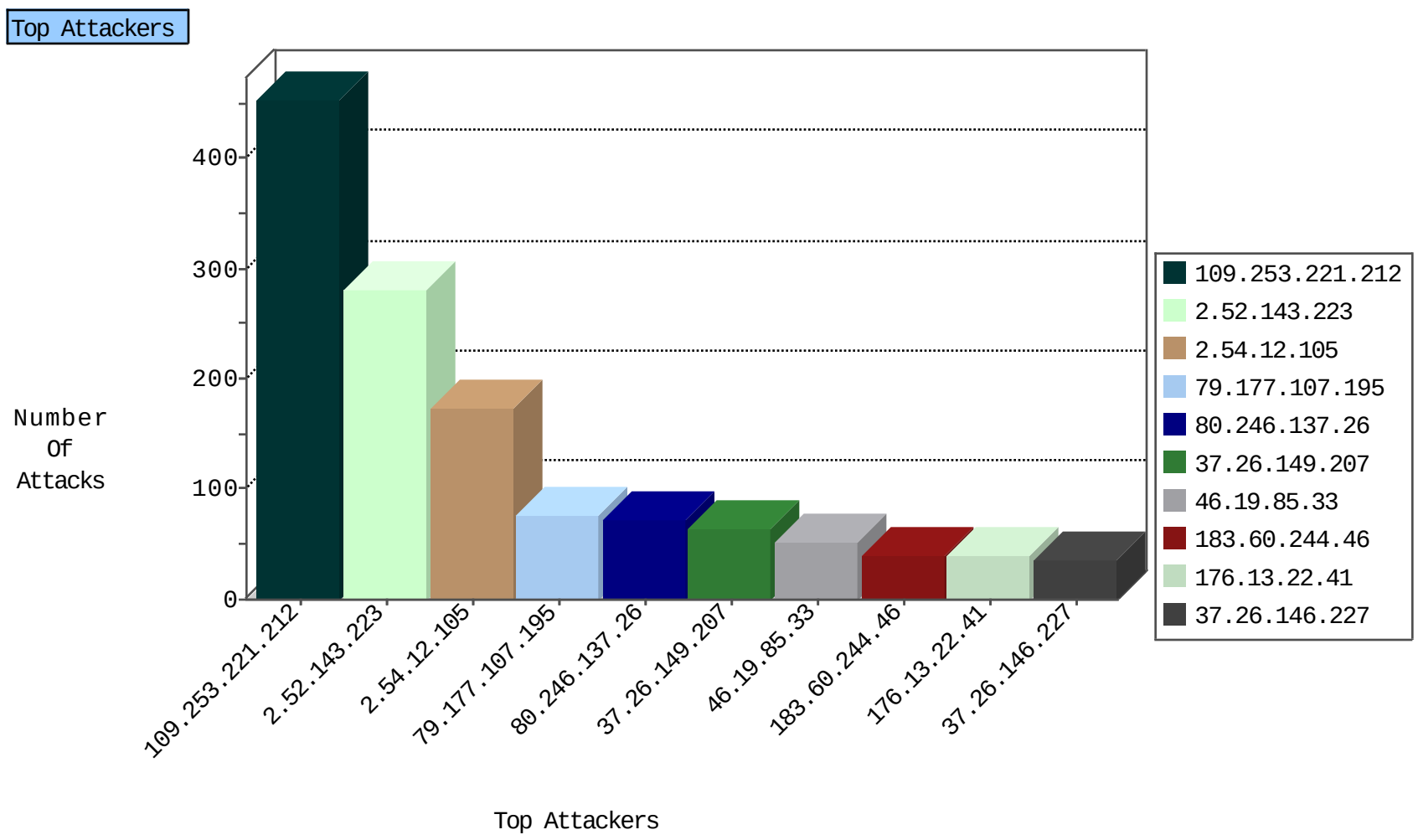
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-08-2016-16:04:09 to 02-08-2016-17:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
158.169.40.9	Belgium	147.237.77.176	matpash.idf.il	Frk_Purple_Con_Limit_Http	drop	3
37.142.64.28	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
149.78.113.47	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	3
158.169.40.9	Belgium	147.237.77.176	matpash.idf.il	Frk_Under_Attack_Con_Http	drop	2

02-08-2016-16:04:09 to 02-08-2016-17:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
69.175.117.202	United States	147.237.77.170	maarachot.idf.il	C123: ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 1	Block	1
162.210.196.98	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1

02-08-2016-16:04:09 to 02-08-2016-17:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.12.105	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	76
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
109.67.10.214	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
109.186.135.119	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
54.67.38.74	147.237.72.167	United States	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
109.64.192.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.45.137.67	147.237.72.217	Turkey	e.idf.il	ET SCAN NMAP -sS window 1024	1
94.230.85.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.232	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.139.23.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.17.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.101.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.50.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
109.201.154.210	147.237.8.27	Netherlands	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
49.143.32.8	147.237.77.243	Korea, Republic of	mobile.idf.il	ET SCAN Potential SSH Scan	1
95.86.97.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.253.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.51.30	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.212.101	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.53.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
109.253.202.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-08-2016-16:04:09 to 02-08-2016-17:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.12.105	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	66
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
46.19.86.68	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
46.19.86.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
89.139.224.212	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.143.223	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.198.151.45	Europe	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	11
95.35.16.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
2.54.174.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
95.221.241.146	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	10
5.36.56.114	Oman	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
2.54.12.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.198.151.43	Europe	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	7
5.36.56.114	Oman	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.54.12.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.22.130.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.102.169.113	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.168.144.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.10.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.12.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
87.68.147.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.130.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
79.182.166.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.135.102.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.235.96.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.12.105	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
87.69.37.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.14.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.28.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.54.174.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.174.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.174.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
68.119.73.222	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.67.170.241	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
37.46.39.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
158.169.40.9	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
5.22.129.66	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.3	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.61.94	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.41.190.175	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.125.13.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.193.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.239	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

02-08-2016-16:04:09 to 02-08-2016-17:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.221.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	280
2.52.143.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	142
2.52.143.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
109.253.221.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
79.177.107.195	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	76
80.246.137.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
37.26.149.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
46.19.85.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
109.253.221.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	48
176.13.22.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
37.26.146.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
2.54.37.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
183.60.244.46	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 183.60.244.46	Block	25
46.19.86.245	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
79.178.182.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
183.60.244.46	China	147.237.77.170	maarachot.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
188.143.232.10	Russian Federation	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker	Block	7
183.60.244.46	China	147.237.77.170	maarachot.idf.il	Distributed Admin Blocking	Block	7
46.19.86.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
79.178.182.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
188.143.232.11	Russian Federation	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker	Block	4
2.54.164.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.218.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.134.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.139.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
68.119.73.222	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.119.73.222	Block	2
109.253.215.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.178.87.95	Oman	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1086-23138-he/dover.aspxbh	Block	2
188.143.232.40	Russian Federation	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker	Block	2
87.69.111.214	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
93.172.231.176	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
95.86.106.182	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
37.142.200.28	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Malformed URL	Block	1
128.232.110.28	United Kingdom	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
46.117.167.76	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	NULL Character in Method Â§[Ã?Ã…XÂ¤0:Â·ÂžÂ‹ OJ*uHÂ´[[#23]]8Â¨+[[#4]]Â™ÃƒÂ¶Ã½jÂ¦[[#0]]2wÂ¾Ã³iD ÃªÃŠÂ…Â¥[[#5]]'Ã—Â±Ã?Ã²[[#4]]>Ã¤Ã…[[#27]]8Ã¨Ã¿Ã'mÂ‹ Â³Vn[[#29]]Ã‡	Block	1
109.160.148.95	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
87.68.40.239	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Malformed URL :×¨ÂžÂ¯6Â¿x*[z[[#21]]Ã»fÂ¥[[#4]]Â¥Â¿Ã·â€œ Ã?d,pâ€°	Block	1
207.46.13.54	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
149.88.224.67	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
104.131.98.84	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
2.54.153.176	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Unknown HTTP Request Method M#Ã—UÂ²Ãœ(ÂªFÂ®Â«ÂšÂ¼Ã„ Ã´Ã?ÃŒS5Ã•Â„Â?Ã-[[#26]][[#3]]Âœ]Â“ Ãºx%`[[#11]]<Ã©Ã¦}Y[[#15]]vÃ±ÃŸ in URL	Block	1
81.218.153.228	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1

02-08-2016-16:04:09 to 02-08-2016-17:04:09