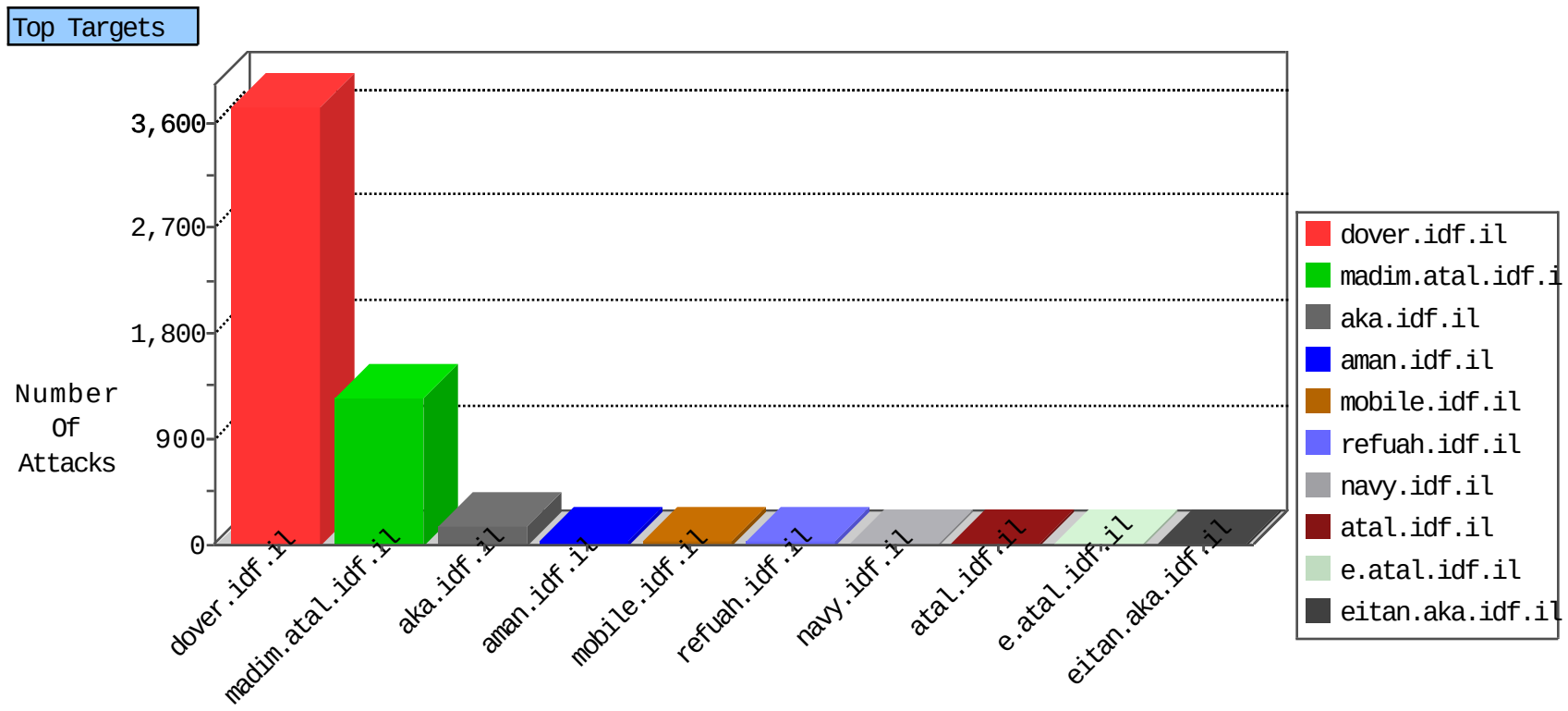
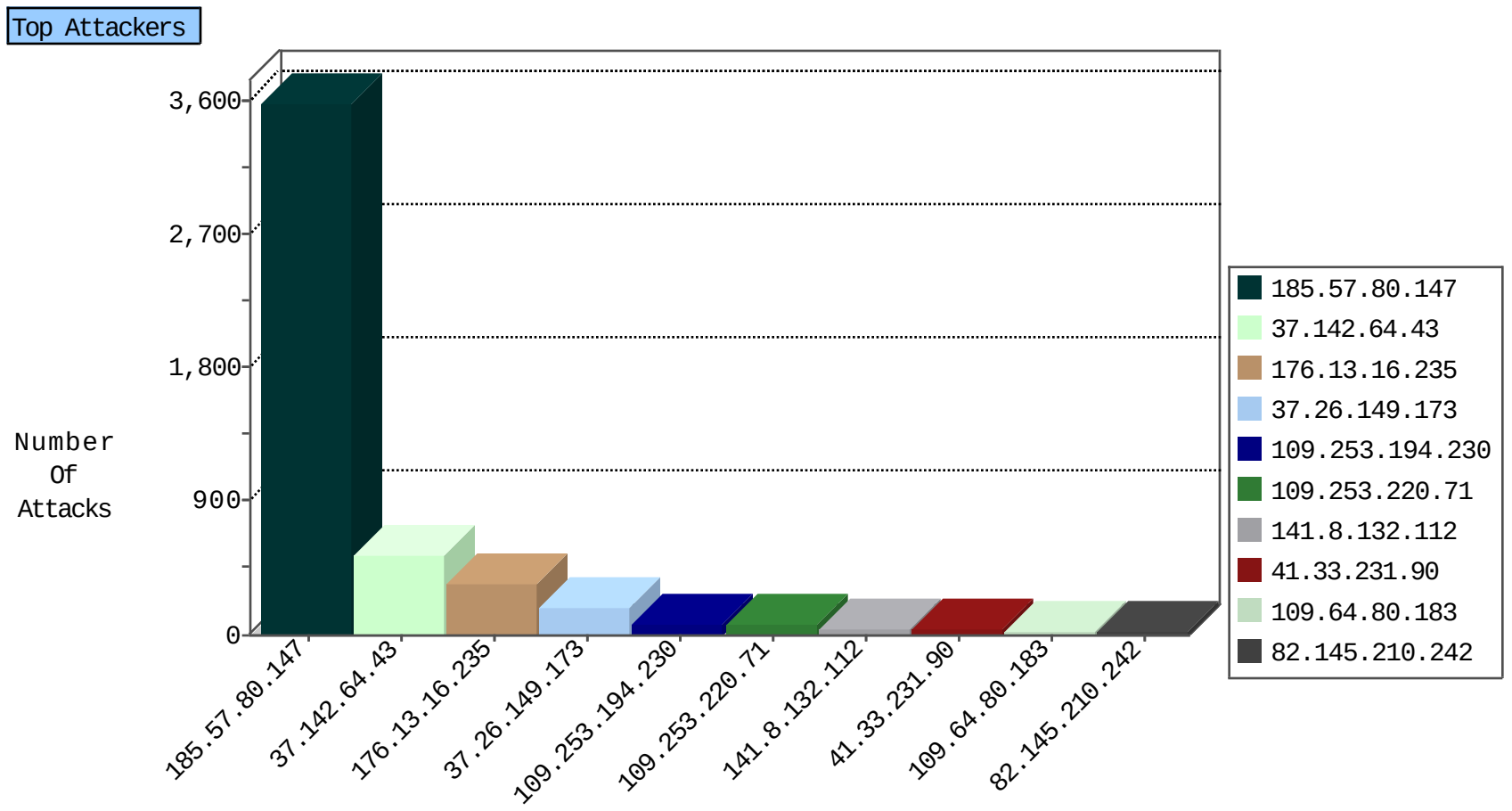
02-17-2016-07:04:05 to 02-17-2016-08:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-17-2016-07:04:05 to 02-17-2016-08:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.173	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
192.99.194.128	Canada	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.10	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
196.200.16.200	Kenya	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1
185.130.5.201		147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
64.110.129.208		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
159.122.252.41	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.201		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
41.206.63.130	Kenya	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1
104.238.129.180		147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
41.206.63.133	Kenya	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1

02-17-2016-07:04:05 to 02-17-2016-08:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-17-2016-07:04:05 to 02-17-2016-08:04:05

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
107.184.234.104	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.62.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.173	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
185.72.179.1	147.237.76.200		eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
185.72.179.1	147.237.0.34		tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
185.72.179.1	147.237.0.34		tikshuv.idf.il	ET SCAN NMAP -f -sS	1
114.112.90.54	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.8.46	Turkey	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.54.90.200	147.237.77.233	United States	atal.idf.il	Tehila - Perl LWP with fake user agent	1
194.187.249.70	147.237.0.16	Europe	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.1	147.237.76.200		eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.1	147.237.0.34		tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
185.57.80.147	147.237.77.216	Romania	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

02-17-2016-07:04:05 to 02-17-2016-08:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
185.57.80.147	Romania	147.237.77.216	dover.idf.il	drop	SAM rule	drop	55
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	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
82.145.210.242	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
46.19.85.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
109.64.80.183	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	15
109.64.80.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	14
85.130.244.74	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.61	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.184	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.88.15.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.148.165	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
84.109.240.51	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.142.68.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.93.56	Israel	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
84.228.62.113	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
62.128.48.50	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
66.249.93.252	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
157.55.12.89	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.94.97.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.10.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.115.144	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
176.13.13.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.115.144	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.67.66.3	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.56	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
212.199.169.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.41.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.126.151.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.1.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.164.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.8.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.252	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
79.182.55.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.194.230	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.139.194	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
2.52.166.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
80.246.139.194	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
192.185.4.108	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
37.26.149.173	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	2
80.246.139.194	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
80.246.139.194	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.46.41.129	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
108.167.133.30	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2

02-17-2016-07:04:05 to 02-17-2016-08:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.57.80.147	Block	1915
37.142.64.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	343
176.13.16.235	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.16.235	Block	185
37.142.64.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
176.13.16.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
37.26.149.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	85
37.26.149.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	80
37.142.64.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	78
109.253.194.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	75
109.253.220.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	71
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1824-he/dover.aspx	Block	60
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1781-he/dover.aspx	Block	60
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1785-he/dover.aspx	Block	60
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1415-he/dover.aspx	Block	60
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucNewsFlashControl$datepicker in www.idf.il/1153-he/dover.aspx	Block	60
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1779-he/dover.aspx	Block	60
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1133-he/dover.aspx	Block	60
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1815-he/dover.aspx	Block	60
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucNewsFlashControl$datepicker in www.idf.il/1841-he/dover.aspx	Block	60
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1362-he/dover.aspx	Block	59
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1806-he/dover.aspx	Block	59
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1380-he/dover.aspx	Block	59
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1384-he/dover.aspx	Block	58
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1381-he/dover.aspx	Block	58
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1361-he/dover.aspx	Block	58
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1379-he/dover.aspx	Block	57
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1842-he/dover.aspx	Block	56
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1129-he/dover.aspx	Block	55
176.13.16.235	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.16.235	Block	52
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1837-he/dover.aspx	Block	50
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1780-he/dover.aspx	Block	50
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1383-he/dover.aspx	Block	49
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1129-he/dover.aspx	Block	30
185.32.179.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	20
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation tab in www.idf.il/1129-he/dover.aspx	Block	16
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1815-he/dover.aspx	Block	10
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1361-he/dover.aspx	Block	10
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1379-he/dover.aspx	Block	10
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1779-he/dover.aspx	Block	10
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	10
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1380-he/dover.aspx	Block	10
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	10
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1781-he/dover.aspx	Block	10
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1815-he/dover.aspx	Block	10
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	10

02-17-2016-07:04:05 to 02-17-2016-08:04:05

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1824-he/dover.aspx	Block	10
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	10
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1129-he/dover.aspx	Block	10
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1362-he/dover.aspx	Block	10

02-17-2016-07:04:05 to 02-17-2016-08:04:05