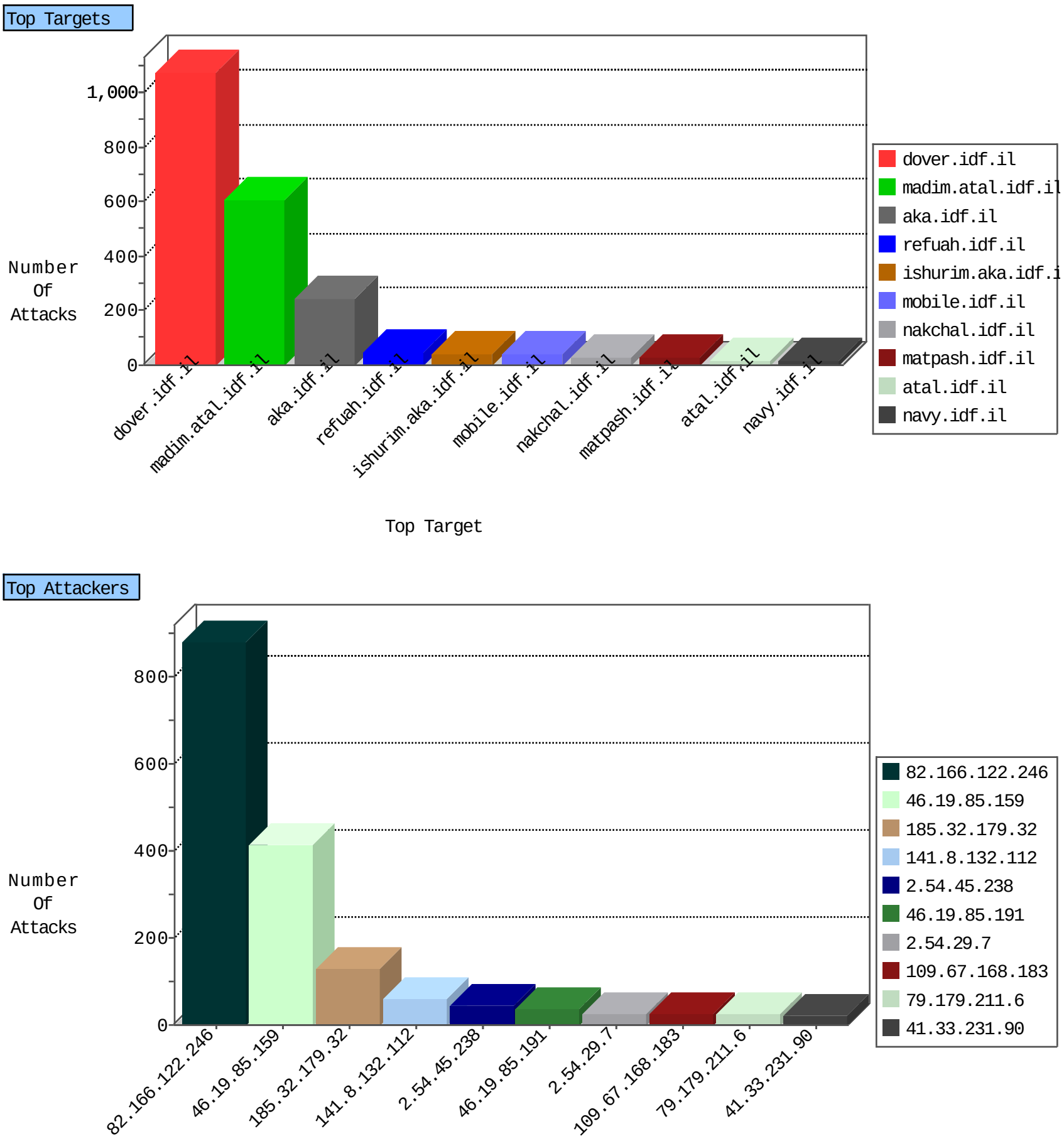
02-14-2016-20:04:01 to 02-14-2016-21:04:01

IDF Under Attack Daily Report



02-14-2016-20:04:01 to 02-14-2016-21:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.228.143.250	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
95.86.109.248	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
185.130.5.201		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
82.166.122.246	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
185.94.111.1		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

02-14-2016-20:04:01 to 02-14-2016-21:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.3.147.188	Israel	147.237.77.74	law.idf.il	C008: HTTP: Xenu UserAgent	Block	1
41.234.7.141	Egypt	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

02-14-2016-20:04:01 to 02-14-2016-21:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
112.196.49.101	147.237.0.35	India	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
112.196.49.101	147.237.0.35	India	akaws.idf.il	ET SCAN NMAP -f -sS	1
109.253.141.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
107.181.161.138	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.57.34	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
41.234.7.141	147.237.77.216	Egypt	dover.idf.il	GPL WEB_SERVER /etc/passwd	1
5.29.251.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
123.22.163.169	147.237.72.14	Vietnam	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.196.49.101	147.237.0.35	India	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
110.182.0.133	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
107.181.161.138	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.172.140	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
75.147.140.253	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
41.234.7.141	147.237.77.216	Egypt	dover.idf.il	SQL Injection - Select From	1

02-14-2016-20:04:01 to 02-14-2016-21:04:01

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	319
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
46.19.85.191	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
109.67.168.183	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.179.211.6	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
5.28.159.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
31.13.163.55	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.22.135.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
74.6.254.118	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
185.5.60.84	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
84.111.139.124	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.66	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.22.135.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.228.143.250	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
45.79.168.168		147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.146.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.220.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.143.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.29.7	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.29.7	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
37.46.39.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.66	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.29.7	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.130.240.135	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	5
2.54.29.7	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.52.142.170	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.29.7	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
5.22.135.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.64.111.223	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.46.41.51	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.22.135.231	Israel	147.237.77.216	dover.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
79.181.146.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.138.125.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.178.2.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.178.157.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
87.68.75.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.134.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.134.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.210.83	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.248.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.210.24.118	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3

02-14-2016-20:04:01 to 02-14-2016-21:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.159	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.159	Block	208
46.19.85.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	198
185.32.179.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	127
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucNewsFlashControl$datepicker1 in www.idf.il/1841-he/dover.aspx	Block	48
2.54.45.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucNewsFlashControl$datepicker1 in www.idf.il/1153-he/dover.aspx	Block	37
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1133-he/dover.aspx	Block	34
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1361-he/dover.aspx	Block	34
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1129-he/dover.aspx	Block	30
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1815-he/dover.aspx	Block	27
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1362-he/dover.aspx	Block	23
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1842-he/dover.aspx	Block	23
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1380-he/dover.aspx	Block	20
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	20
176.13.11.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
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	18
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1384-he/dover.aspx	Block	18
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1780-he/dover.aspx	Block	17
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1379-he/dover.aspx	Block	15
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1806-he/dover.aspx	Block	14
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1841-he/dover.aspx	Block	13
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1781-he/dover.aspx	Block	13
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucNewsFlashControl$ImageButton1.x in www.idf.il/1153-he/dover.aspx	Block	10
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	10
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1785-he/dover.aspx	Block	9
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucNewsFlashControl$ImageButton1.x in www.idf.il/1841-he/dover.aspx	Block	9
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	8
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1415-he/dover.aspx	Block	7
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.y in www.idf.il/1379-he/dover.aspx	Block	7
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	7
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.x in www.idf.il/1415-he/dover.aspx	Block	7
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1129-he/dover.aspx	Block	6
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1381-he/dover.aspx	Block	6
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1361-he/dover.aspx	Block	5
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.y in www.idf.il/1842-he/dover.aspx	Block	4
46.19.85.159	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.85.159	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.y in www.idf.il/1361-he/dover.aspx	Block	4
176.13.18.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
41.234.7.141	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.234.7.141	Block	3
217.132.41.55	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 217.132.41.55	Block	3
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.y in www.idf.il/1381-he/dover.aspx	Block	3
5.29.102.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
92.96.159.221	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	2

02-14-2016-20:04:01 to 02-14-2016-21:04:01

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.133.193	Israel	147.237.76.31	nakchal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
80.246.136.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.x in www.idf.il/1384-he/dover.aspx	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2

02-14-2016-20:04:01 to 02-14-2016-21:04:01