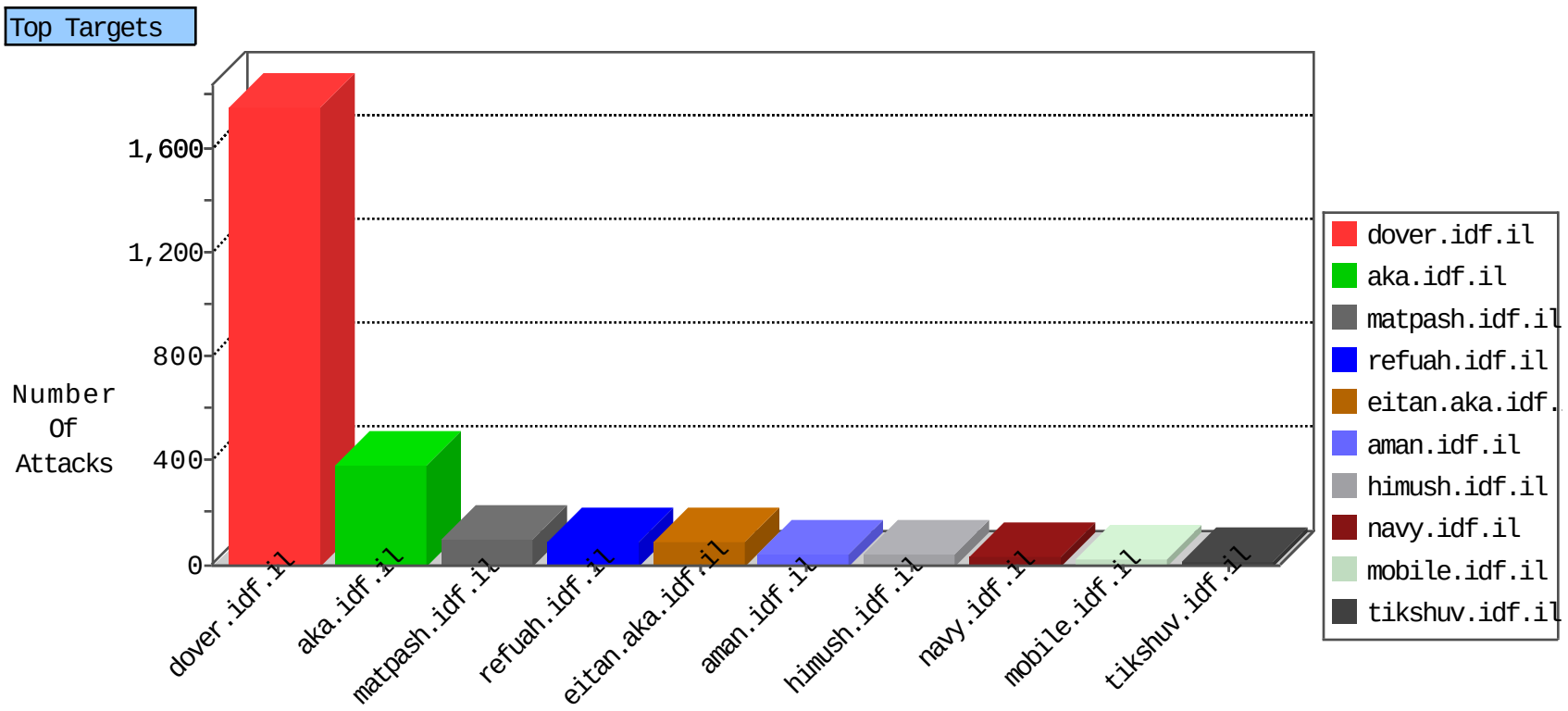
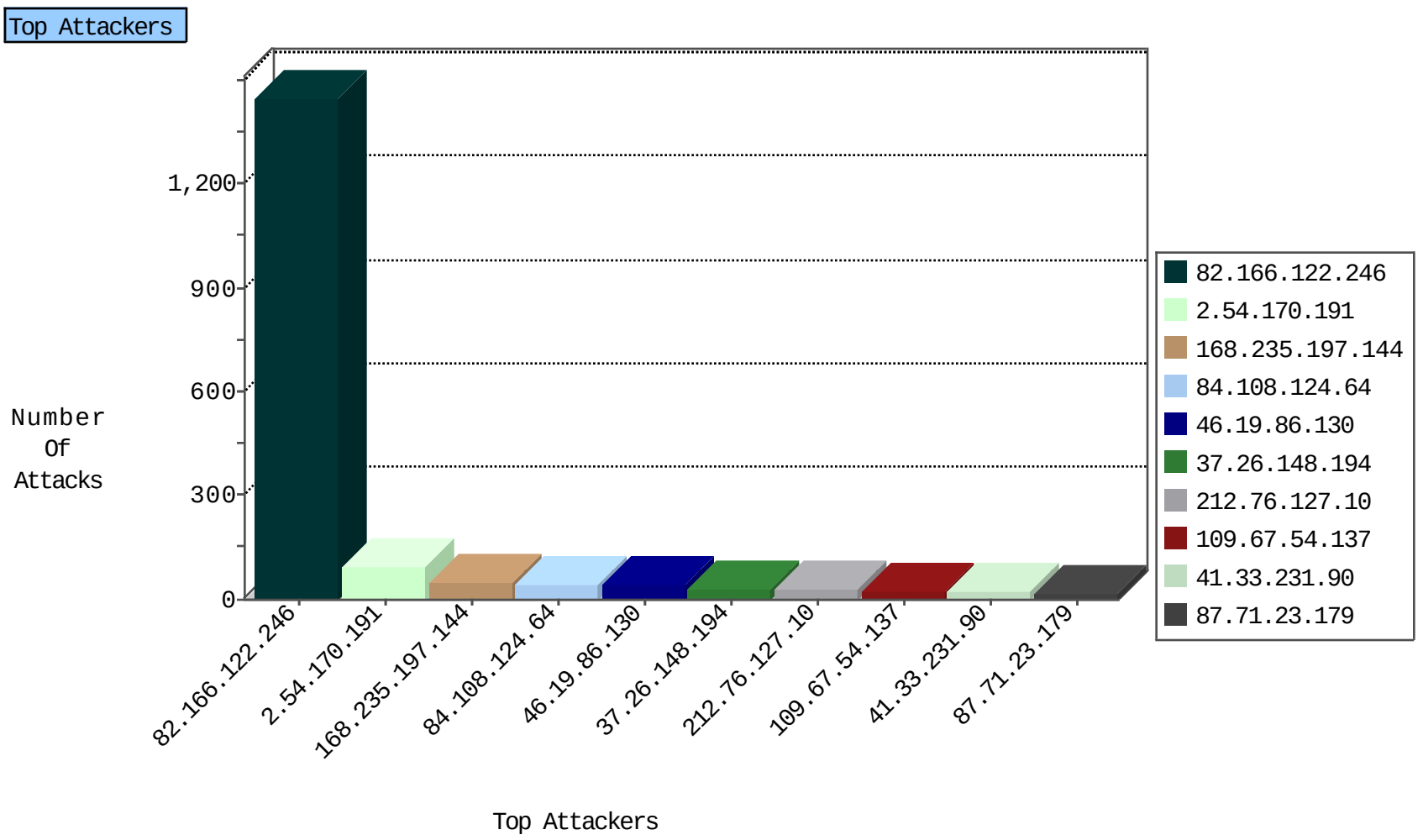
02-14-2016-21:04:07 to 02-14-2016-22:04:07

IDF Under Attack
Daily Report





02-14-2016-21:04:07 to 02-14-2016-22:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
168.235.197.144	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
114.186.10.212	Japan	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.111	Switzerland	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
185.56.28.67	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

02-14-2016-21:04:07 to 02-14-2016-22:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.166.122.246	Israel	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	6
85.251.251.9	Spain	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	2

02-14-2016-21:04:07 to 02-14-2016-22:04:07

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	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	15
82.166.122.246	147.237.77.216	Israel	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	15
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
132.252.173.4	147.237.77.216	Germany	dover.idf.il	GPL SCAN nmap TCP	2
119.81.162.182	147.237.76.176	Hong Kong	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
109.64.160.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.166.122.246	147.237.77.216	Israel	dover.idf.il	tehila expiremental XSS in POST	1
218.246.0.97	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.198.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.76.39	United States	mobile.meitav.idf.il	ET DROP Dshield Block Listed Source	1
183.82.106.200	147.237.76.177	India	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
173.14.248.34	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
119.81.162.182	147.237.76.176	Hong Kong	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
119.81.162.182	147.237.76.176	Hong Kong	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
84.111.233.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.166.122.246	147.237.77.216	Israel	dover.idf.il	SERVER-WEBAPP cross-site scripting attempt via form data attempt	1
218.201.61.82	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
183.82.106.200	147.237.76.177	India	ncore.idf.il	ET SCAN NMAP -f -sS	1

02-14-2016-21:04:07 to 02-14-2016-22:04:07

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	Command Injection		monitor	423
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	318
168.235.197.144	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	48
2.54.170.191	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	39
84.108.124.64	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
212.76.127.10	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	27
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Command Injection	command injection detected in request: 'ls'	monitor	27
82.166.122.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
109.67.54.137	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
85.64.122.228	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
213.8.240.179	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.170.191	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
2.54.170.191	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
2.54.170.191	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	14
5.29.39.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.145	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.180.226.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
176.13.20.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
79.183.32.101	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.71.23.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
87.69.219.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
109.64.184.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.60.47.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
85.250.107.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
176.13.9.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.109.8.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
87.68.69.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
93.172.241.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
46.117.116.108	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
109.253.131.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.131.253	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.33	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.80.134.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.172.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.149.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.130	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.177.170.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.71.23.179	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.130	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.201.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.152.148	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.130	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
79.179.199.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.252.170.22	Italy	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

02-14-2016-21:04:07 to 02-14-2016-22:04:07

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.i	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	168
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucNewsFlashControl$datepicker1 in www.idf.il/1841-he/dover.aspx	Block	20
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucNewsFlashControl$datepicker1 in www.idf.il/1153-he/dover.aspx	Block	18
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1781-he/dover.aspx	Block	16
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1384-he/dover.aspx	Block	16
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1785-he/dover.aspx	Block	16
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1415-he/dover.aspx	Block	16
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1806-he/dover.aspx	Block	16
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1380-he/dover.aspx	Block	16
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1779-he/dover.aspx	Block	16
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1815-he/dover.aspx	Block	16
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1381-he/dover.aspx	Block	16
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1780-he/dover.aspx	Block	12
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1837-he/dover.aspx	Block	12
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1383-he/dover.aspx	Block	12
82.166.122.246	Israel	147.237.77.216	dover.idf.i	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.i	Parameter Type Violation PageNum in www.idf.il/1785-he/dover.aspx	Block	8
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation PageNum in www.idf.il/1384-he/dover.aspx	Block	8
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation PageNum in www.idf.il/1806-he/dover.aspx	Block	8
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation PageNum in www.idf.il/1415-he/dover.aspx	Block	8
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation PageNum in www.idf.il/1815-he/dover.aspx	Block	8
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	8
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation PageNum in www.idf.il/1781-he/dover.aspx	Block	8
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	7
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation PageNum in www.idf.il/1361-he/dover.aspx	Block	7
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	5
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.y in www.idf.il/1381-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.x in www.idf.il/1806-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.y in www.idf.il/1780-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.x in www.idf.il/1779-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.y in www.idf.il/1837-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.y in www.idf.il/1383-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.x in www.idf.il/1815-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.x in www.idf.il/1381-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.y in www.idf.il/1781-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.x in www.idf.il/1780-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.y in www.idf.il/1384-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.x in www.idf.il/1837-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.x in www.idf.il/1383-he/dover.aspx	Block	4

02-14-2016-21:04:07 to 02-14-2016-22:04:07

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.y in www.idf.il/1785-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucNewsFlashControl$ImageButton1.x in www.idf.il/1841-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.x in www.idf.il/1781-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1133-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.y in www.idf.il/1415-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.x in www.idf.il/1384-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.y in www.idf.il/1806-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.x in www.idf.il/1785-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.y in www.idf.il/1779-he/dover.aspx	Block	4
82.166.122.246	Israel	147.237.77.216	dover.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.x in www.idf.il/1415-he/dover.aspx	Block	4
66.249.66.25	Israel	147.237.77.216	dover.idf.i	Multiple Unauthorized URL Access from 66.249.66.25	Block	4

02-14-2016-21:04:07 to 02-14-2016-22:04:07