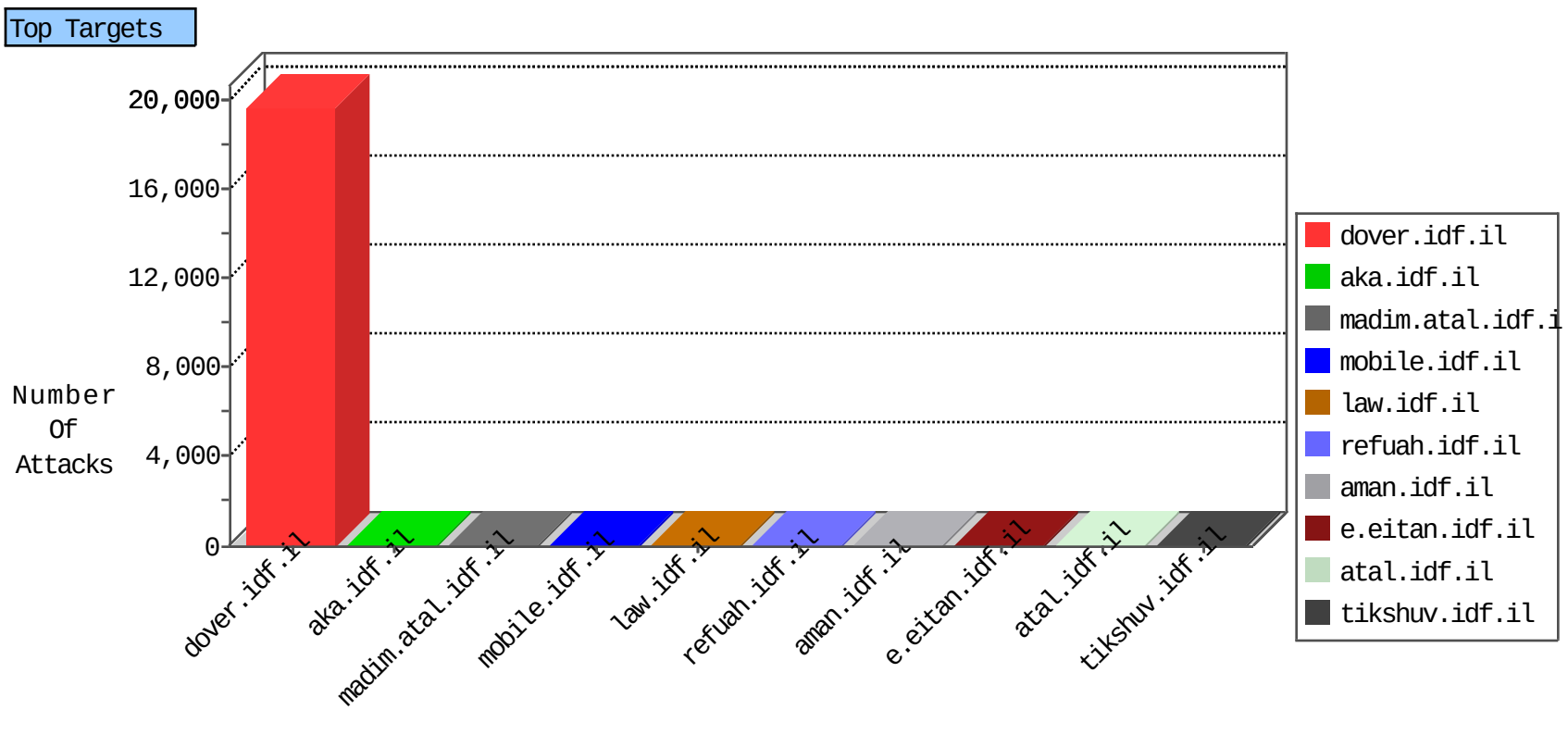
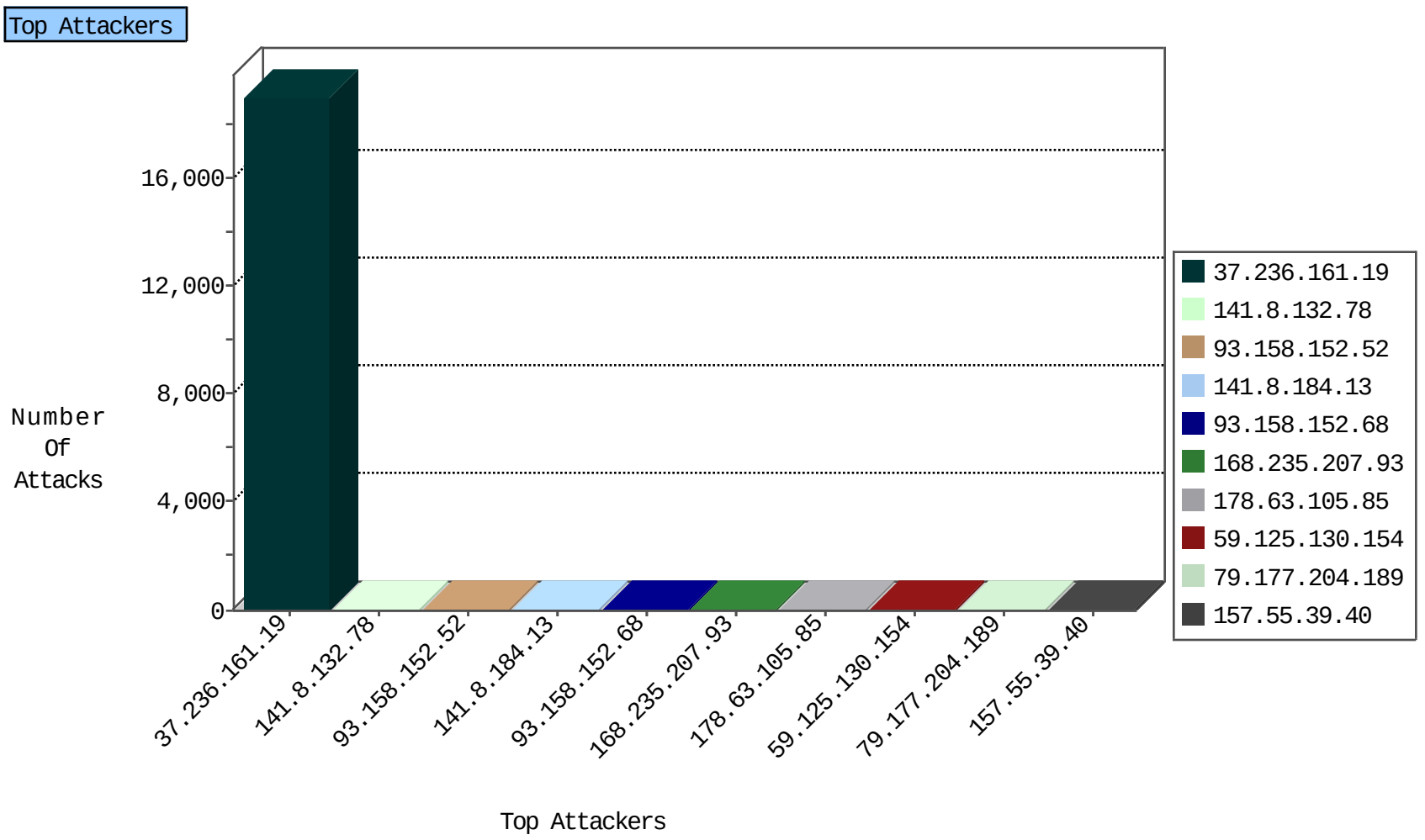
03-07-2016-01:09:39 to 03-07-2016-02:09:39

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-07-2016-01:09:39 to 03-07-2016-02:09:39

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	723
82.145.216.44	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
82.145.216.106	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
168.235.207.93	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
168.235.207.93	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
58.42.230.122	China	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

03-07-2016-01:09:39 to 03-07-2016-02:09:39

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.108	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
81.109.65.38	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	3
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
207.46.13.98	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.132	Italy	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

03-07-2016-01:09:39 to 03-07-2016-02:09:39

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
59.125.130.154	147.237.0.19	Taiwan	madim.atal.idf.il	SERVER-WEBAPP apache directory disclosure attempt	8
59.125.130.154	147.237.0.19	Taiwan	madim.atal.idf.il	GPL WEB_SERVER apache directory disclosure attempt	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
218.57.11.7	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
209.79.65.140	147.237.0.19	United States	madim.atal.idf.il	SERVER-WEBAPP apache directory disclosure attempt	1
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
208.109.53.250	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
208.109.53.250	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
208.109.53.250	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
208.109.53.250	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
80.80.172.182	147.237.76.30	Albania	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.246.0.97	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
218.57.11.7	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
209.79.65.140	147.237.0.19	United States	madim.atal.idf.il	GPL WEB_SERVER apache directory disclosure attempt	1
59.45.79.117	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
208.109.53.250	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
208.109.53.250	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
208.109.53.250	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.244.49.137	147.237.76.42	Hong Kong	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
218.57.11.7	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1

03-07-2016-01:09:39 to 03-07-2016-02:09:39

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17747
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	135
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	76
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	71
141.8.184.13	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
93.158.152.68	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	62
168.235.207.93	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
79.177.204.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Anonymous DoSer Denial of Service Tool	reject	14
157.55.39.40	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
107.170.119.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
46.19.86.72	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
189.114.3.238	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.i	drop	SAM rule	drop	7
141.8.132.95	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.142.68.0	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
178.154.149.6	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.255.253.8	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
130.193.37.10	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.176.208.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
101.2.171.162	Australia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
130.193.37.4	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
130.193.51.62	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
101.2.171.162	Australia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
37.26.149.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
168.235.207.93	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
87.69.62.195	Israel	147.237.0.34	tikshuv.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
213.57.37.8	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.65.233.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.2.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.37.8	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
189.46.234.86	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
31.210.187.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.i	drop	SAM rule	drop	3
79.183.193.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	3
2.25.233.78	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.196.167.8	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.8.142.89	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
93.35.221.212	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
131.181.158.20	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
61.135.189.108	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2

03-07-2016-01:09:39 to 03-07-2016-02:09:39

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 37.236.161.19	Block	193
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
66.249.64.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
45.35.105.129		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
17.138.56.26	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	2
77.224.7.171	Spain	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
77.224.7.171	Spain	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	2
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
100.15.103.50	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.231.40	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	1
66.249.64.51	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery.nyromodal-1.6.2.js	Block	1
196.221.237.247	Egypt	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
157.55.39.52	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
82.221.22.64	Iceland	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
207.241.229.222	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.66.36	United States	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
189.114.3.238	Brazil	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/&prev=search	Block	1
62.90.215.148	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
101.2.171.162	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.56	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
196.221.237.247	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
172.98.86.21		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
82.221.22.64	Iceland	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/components/com_contushdvideoshare/hdflvplayer/download.php	Block	1
66.249.66.182	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
196.221.237.247	Egypt	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
104.236.231.135		147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/magento_version	Block	1
66.249.64.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
196.221.237.247	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
172.98.86.21		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
40.77.167.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
87.69.158.111	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
196.221.237.247	Egypt	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/xmlrpc.php	Block	1
112.204.199.239	Philippines	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
79.176.55.240	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
196.221.237.247	Egypt	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
180.76.15.6	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8944-he/refuah.aspx	Block	1
87.69.158.111	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
66.102.7.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
196.221.237.247	Egypt	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
112.204.199.239	Philippines	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	1
79.176.55.240	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
196.221.237.247	Egypt	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
66.249.64.235	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
180.76.15.159	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
45.50.179.44		147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1

03-07-2016-01:09:39 to 03-07-2016-02:09:39