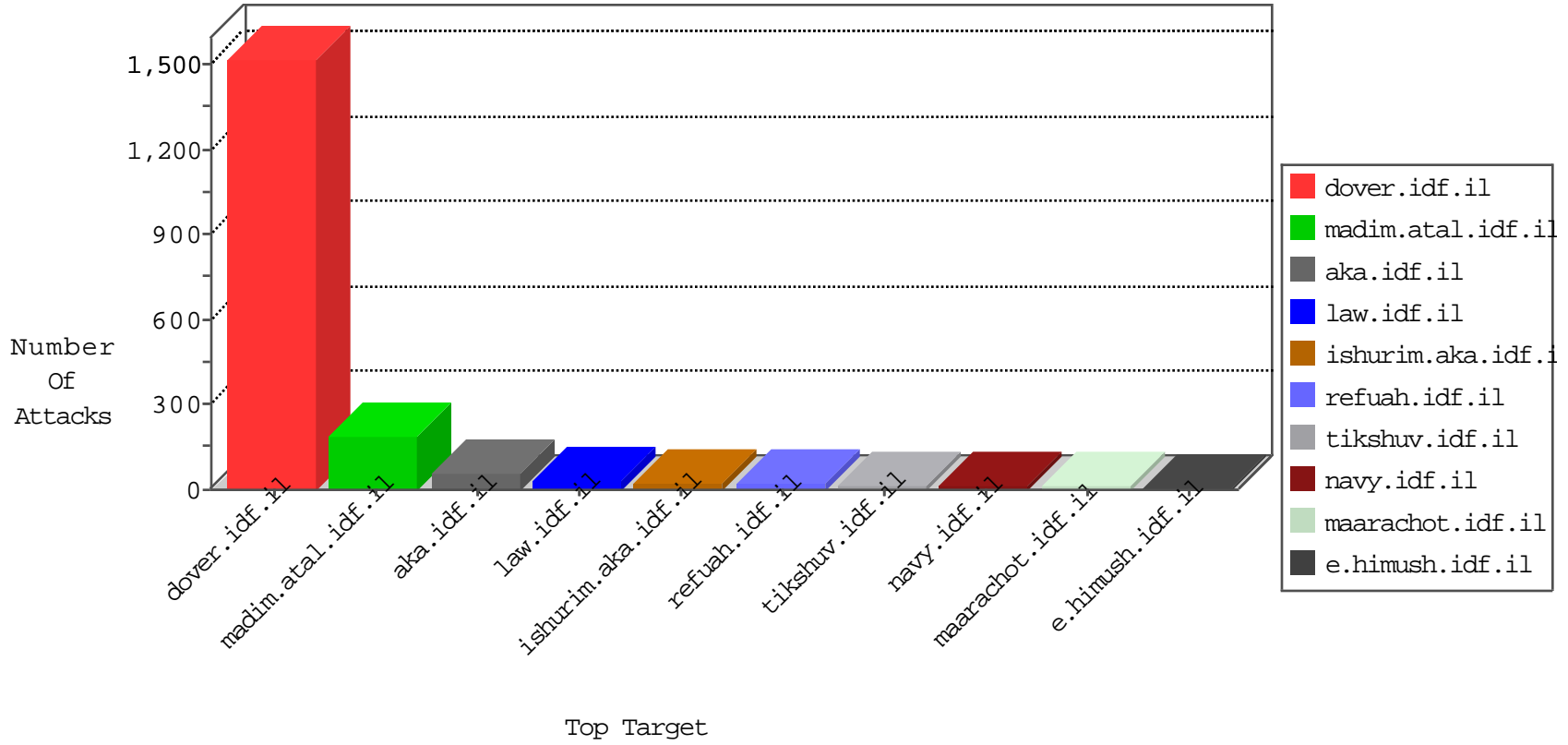


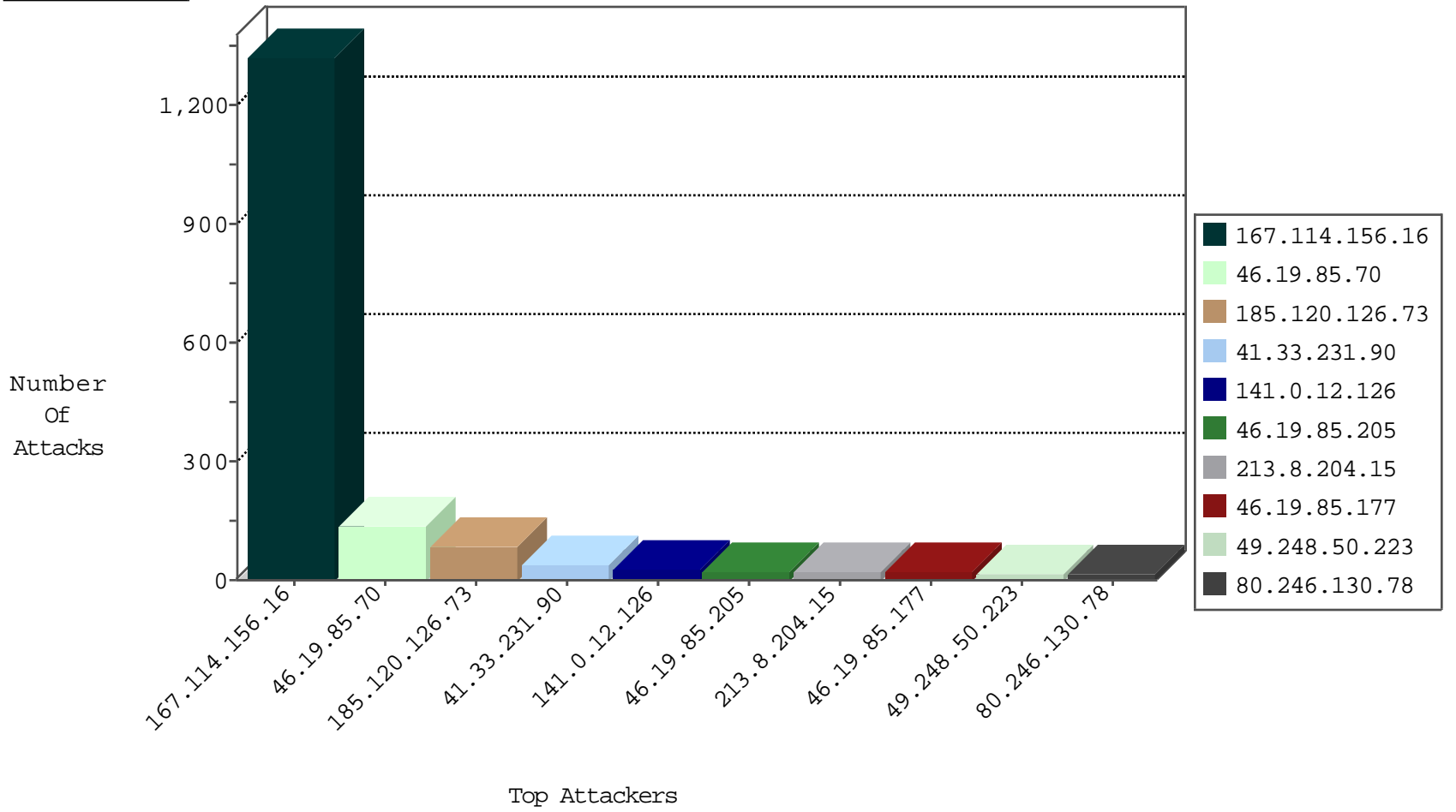
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3982
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3510
79.182.114.82	Israel	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	3
79.182.114.82	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
82.221.105.7	Iceland	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
45.58.118.218		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
123.195.128.69	Taiwan	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
45.58.118.218		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

01-06-2016-06:04:08 to 01-06-2016-07:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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	3
80.82.69.91	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
117.25.155.164	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
117.25.155.164	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
104.128.144.131	147.237.8.24	Canada	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
93.174.93.203	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.100.85.148	147.237.76.197		e.himush.idf.il	ET SCAN Potential SSH Scan	1
117.25.155.164	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
106.75.199.201	147.237.76.177	China	ncore.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
104.128.144.131	147.237.8.24	Canada	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	27
141.0.12.126	Norway	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	25
49.248.50.223	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.177	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.205	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.177	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.205	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.12.134.10	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.13	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.7	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
40.77.167.95	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
91.200.12.7	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	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
46.19.85.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
2.54.19.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.13	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.216	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
40.77.167.43	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.66.95	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
178.62.162.228	United Kingdom	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
157.55.39.127	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
40.77.167.43	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.127.107.108	Netherlands	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
5.29.170.134	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
1.39.37.54	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
141.212.121.171	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.122	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
180.97.106.37	China	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.221	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
106.75.199.201	China	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
157.55.39.119	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.94	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
81.169.237.146	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
141.212.121.175	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.121.170	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.72	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.70	Block	59
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.70	Block	33
213.8.204.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
80.246.130.78	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.130.78	Block	14
109.253.195.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
46.19.86.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
109.253.145.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.253.205.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.197.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.21.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
91.143.80.201	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	2
173.252.88.91	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.228.46.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
31.13.102.119	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.65.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1401-he/atal.aspx	Block	1
185.3.147.216	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
216.218.206.68	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
157.55.39.116	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.65.181	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
5.29.164.192	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
176.13.13.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
5.255.253.75	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1414-he/dover.aspx	Block	1