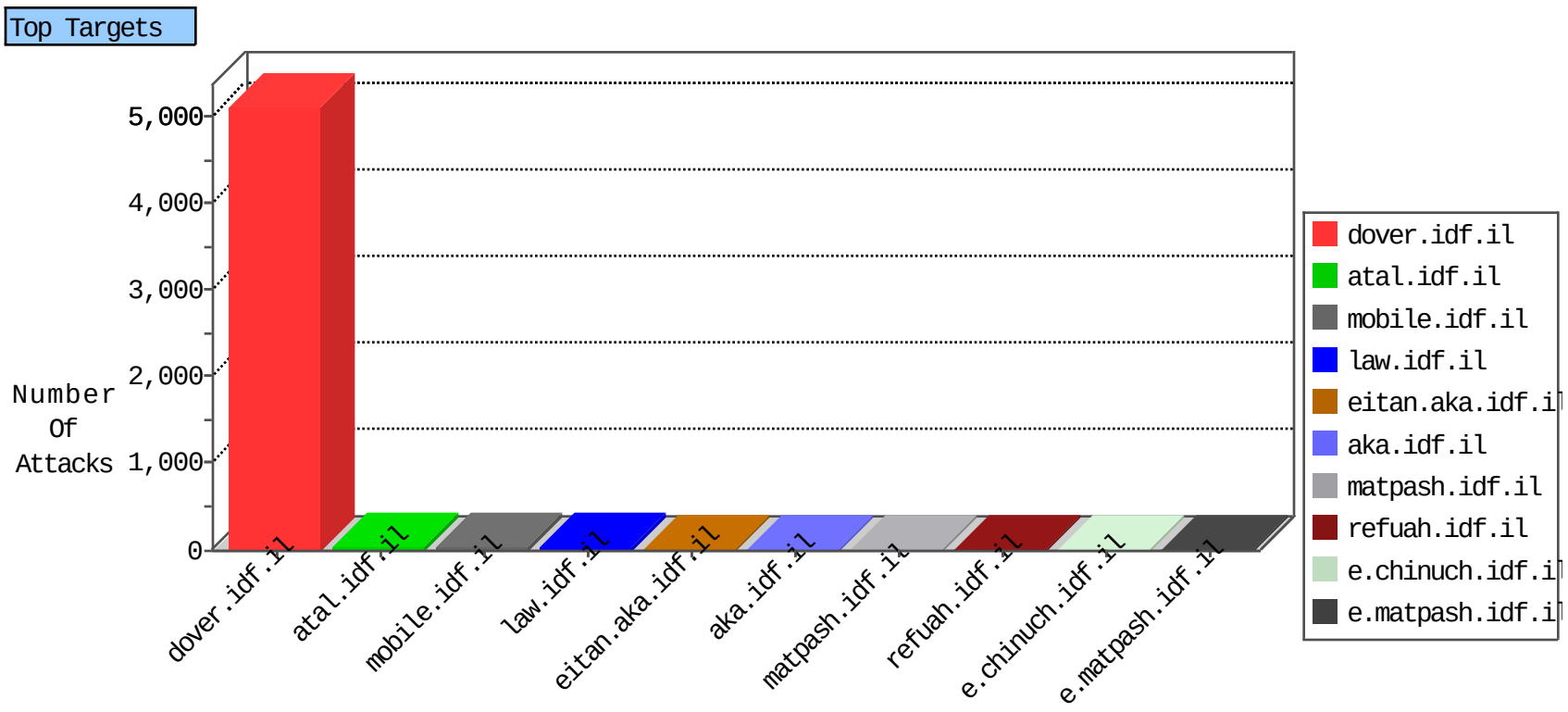
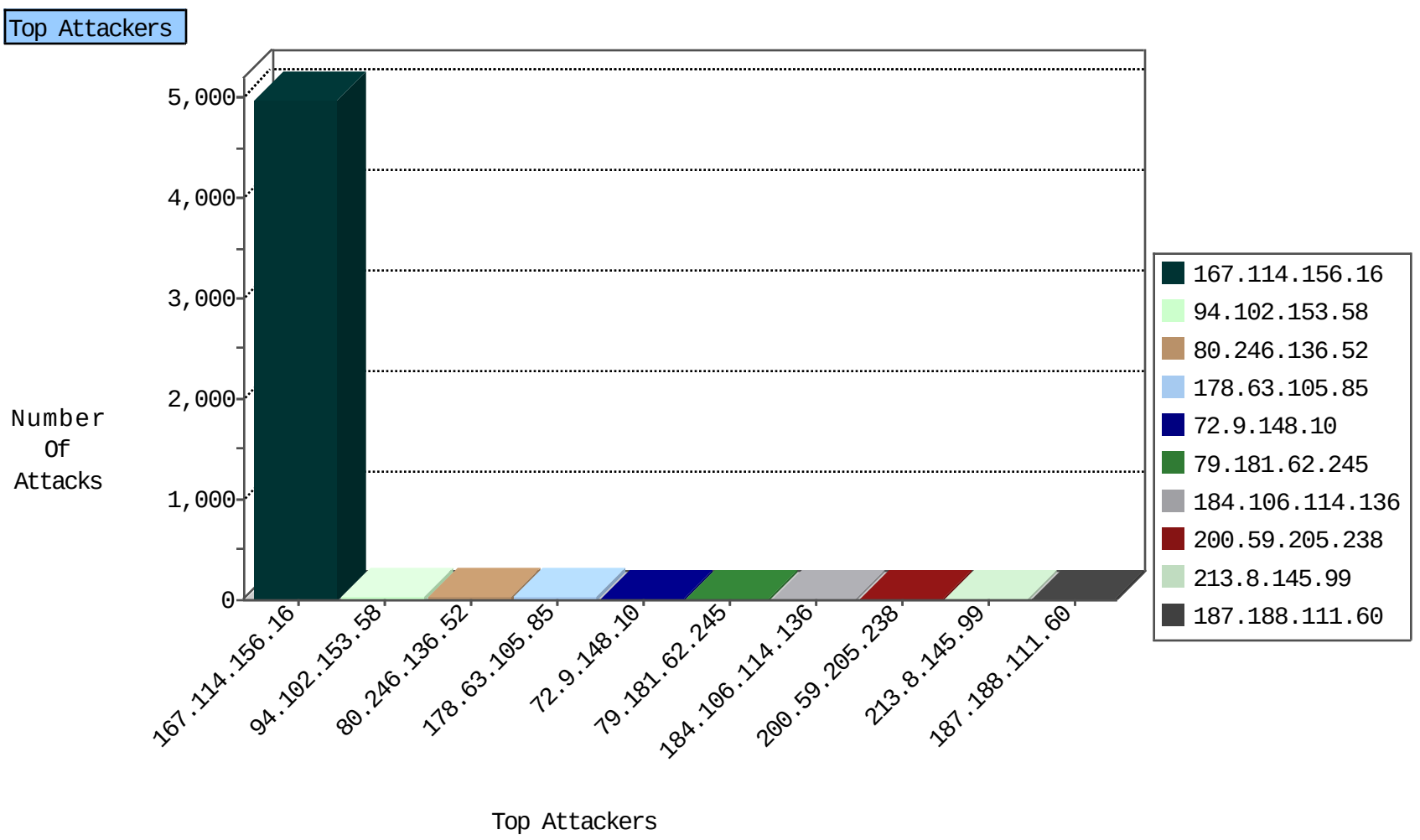
03-13-2016-02:04:06 to 03-13-2016-03:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-13-2016-02:04:06 to 03-13-2016-03:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	9932

03-13-2016-02:04:06 to 03-13-2016-03:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.106.114.136	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
94.102.153.58	United Kingdom	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
184.168.193.34	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
216.185.43.135	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
94.102.153.58	United Kingdom	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
184.173.233.226	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
200.59.205.238	Argentina	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
64.31.44.6	United States	147.237.77.176	matpash.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
213.8.145.99	Israel	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	3
62.210.148.247	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
213.8.145.99	Israel	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

03-13-2016-02:04:06 to 03-13-2016-03:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.102.153.58	147.237.77.216	United Kingdom	dover.idf.il	SQL Injection - Select From	24
213.8.145.99	147.237.77.233	Israel	atal.idf.il	SQL Injection - Select From	12
200.59.205.238	147.237.77.74	Argentina	law.idf.il	SQL Injection - Select From	12
184.106.114.136	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	10
184.173.233.226	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	6
64.31.44.6	147.237.77.176	United States	matpash.idf.il	SQL Injection - Select From	6
216.185.43.135	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
184.168.193.34	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
178.63.11.208	147.237.76.198	Germany	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
115.29.138.97	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
54.67.31.31	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 4096	1
203.115.196.137	147.237.77.205	Malaysia	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
54.67.31.31	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -f -sS	1
13.75.95.104	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
185.100.87.50	147.237.77.178		e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
13.75.95.104	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
178.63.11.208	147.237.76.202	Germany	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
178.63.11.208	147.237.8.24	Germany	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
61.182.170.38	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
54.67.31.31	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 2048	1
50.193.61.77	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
192.3.9.122	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential SSH Scan	1
13.75.95.104	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1

03-13-2016-02:04:06 to 03-13-2016-03:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2164
80.246.136.52	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.181.62.245	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
67.80.113.5	United States	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	4
141.0.15.123	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	4
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	3
185.120.239.23		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	3
185.120.239.23		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	3
87.70.99.192	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.33	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
185.120.239.23		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.98	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	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	3
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	2
157.55.39.134	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
103.238.131.212	Australia	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	2
212.143.38.222	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
41.176.169.22	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
141.212.122.226	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
187.188.111.60	Mexico	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.120.239.23		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1
41.176.169.22	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
187.188.111.60	Mexico	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
187.188.111.60	Mexico	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.63.105.85	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
5.22.130.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
178.63.105.85	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
211.162.33.75	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.228	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
187.188.111.60	Mexico	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.120.239.23		147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
41.176.169.22	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
187.188.111.60	Mexico	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
137.226.113.7	Germany	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
187.188.111.60	Mexico	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
70.35.197.33	United States	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
31.168.147.155	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
178.63.105.85	Germany	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
141.212.122.240	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

03-13-2016-02:04:06 to 03-13-2016-03:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.52	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1749	Block	5
112.109.150.75	China	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 112.109.150.75	Block	4
66.249.82.94	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.52.45.16	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	3
66.249.82.88	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.17.15	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.17.15	Block	2
77.243.183.75	Europe	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/templates/sendtofriend/sendtofriend.aspx parameter l	Block	1
66.249.82.91	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.54.17.15	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	1
140.115.111.116	Taiwan	147.237.72.166	aka.idf.il	Unknown Parameter service in www.aka.idf.il/brothers/klali/default.asp	None	1
66.249.83.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
62.33.84.91	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
68.180.228.151	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout2.css	Block	1
66.249.82.94	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
62.33.84.91	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
157.55.39.112	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
68.180.230.87	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/print.css	Block	1
112.109.150.75	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.83.155	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/107656.pdf	Block	1
198.20.69.74	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
77.243.183.75	Europe	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/templates/sendtofriend/sendtofriend.aspx parameter f	Block	1
140.115.111.116	Taiwan	147.237.72.166	aka.idf.il	Unknown Parameter request in www.aka.idf.il/brothers/skira/default.asp	None	1
66.249.83.158	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
204.79.180.221	United States	147.237.72.167	ishurim.aka.idf.i	SSL Untraceable Connection - Open Mode	None	1

03-13-2016-02:04:06 to 03-13-2016-03:04:06