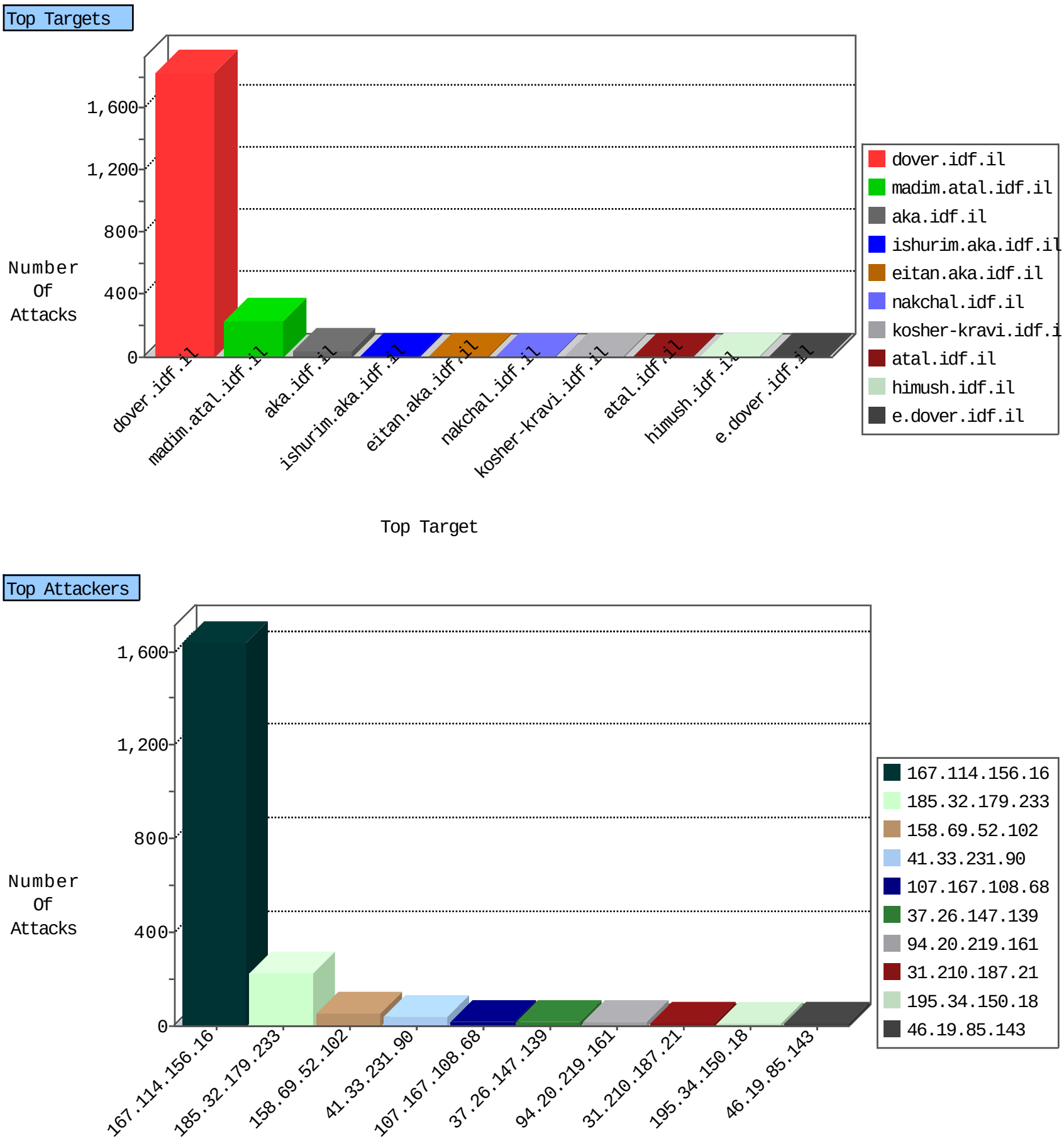
01-04-2016-05:04:09 to 01-04-2016-06:04:09

IDF Under Attack Daily Report



01-04-2016-05:04:09 to 01-04-2016-06:04:09

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	3021
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	34
77.247.178.132	Netherlands	147.237.76.176	test.ncore.idf.i	Block_Ntp_All_Net	drop	1
77.247.178.132	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

01-04-2016-05:04:09 to 01-04-2016-06:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-04-2016-05:04:09 to 01-04-2016-06:04:09

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	4
94.20.219.161	147.237.0.15	Azerbaijan	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
94.20.219.161	147.237.76.147	Azerbaijan	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
94.20.219.161	147.237.8.50	Azerbaijan	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
194.165.155.114	147.237.77.205	Jordan	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
194.165.155.114	147.237.76.34	Jordan	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
88.249.106.23	147.237.0.16	Turkey	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
94.20.219.161	147.237.77.233	Azerbaijan	atal.idf.il	ET SCAN Potential SSH Scan	1
94.20.219.161	147.237.77.212	Azerbaijan	e.dover.idf.il	ET SCAN Potential SSH Scan	1
94.20.219.161	147.237.77.176	Azerbaijan	matpash.idf.il	ET SCAN Potential SSH Scan	1
94.20.219.161	147.237.76.38	Azerbaijan	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
200.225.21.91	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.20.219.161	147.237.76.30	Azerbaijan	himush.idf.il	ET SCAN Potential SSH Scan	1
194.165.155.114	147.237.77.205	Jordan	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
94.20.219.161	147.237.0.200	Azerbaijan	m4u.idf.il	ET SCAN Potential SSH Scan	1
194.165.155.114	147.237.77.178	Jordan	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
93.174.93.203	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
185.32.179.233	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
80.82.69.146	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
94.20.219.161	147.237.77.216	Azerbaijan	dover.idf.il	ET SCAN Potential SSH Scan	1
94.20.219.161	147.237.77.179	Azerbaijan	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
94.20.219.161	147.237.76.202	Azerbaijan	e.halag.idf.il	ET SCAN Potential SSH Scan	1
94.20.219.161	147.237.76.44	Azerbaijan	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
94.20.219.161	147.237.76.31	Azerbaijan	nakchal.idf.il	ET SCAN Potential SSH Scan	1

01-04-2016-05:04:09 to 01-04-2016-06:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
158.69.52.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	53
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
107.167.108.68	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
37.26.147.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
31.210.187.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
24.171.140.55	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
157.55.39.129	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
181.66.3.98	Peru	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	5
66.249.81.212	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	4
46.19.85.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.183.240.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.176.185	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
8.37.235.225	United States	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
65.19.138.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.167.47	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
158.69.52.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.181	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.224		147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
100.33.83.189	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
68.3.160.42	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.98	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.92	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
108.27.52.163	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
79.182.18.221	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.224		147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
101.198.159.31	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.22	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.110	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.124	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
14.121.183.173	China	147.237.76.200	eitan.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
149.78.186.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.224		147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
173.54.56.233	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
103.41.63.11		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.36	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.124	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.203	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
24.163.36.30	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
82.118.236.248	Bulgaria	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
173.54.56.233	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
103.41.63.11		147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
74.82.47.46	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.251	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

01-04-2016-05:04:09 to 01-04-2016-06:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.233	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 185.32.179.233	Block	120
185.32.179.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
109.253.156.92	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
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	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
79.179.34.18	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
66.249.79.234	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/general.aspx	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
149.88.168.188	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 149.88.168.188	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
14.121.183.173	China	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/	None	1
185.32.179.233	Israel	147.237.0.19	madim.atal.idf.i	Too Many 404: Response Code per Session	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../../images/infocenteritem/browser.png	Block	1
157.55.39.129	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
14.121.183.173	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/usercontrols/headerupper/	Block	1
157.55.39.160	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
79.176.185.164	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/personalentrance.asp	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	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	Parameter Type Violation PageNum in www.idf.il/1815-he/dover.aspx	Block	1
157.55.39.205	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/library/manage/resource/getfilecontent.hh.asp	Block	1
79.178.104.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1

01-04-2016-05:04:09 to 01-04-2016-06:04:09