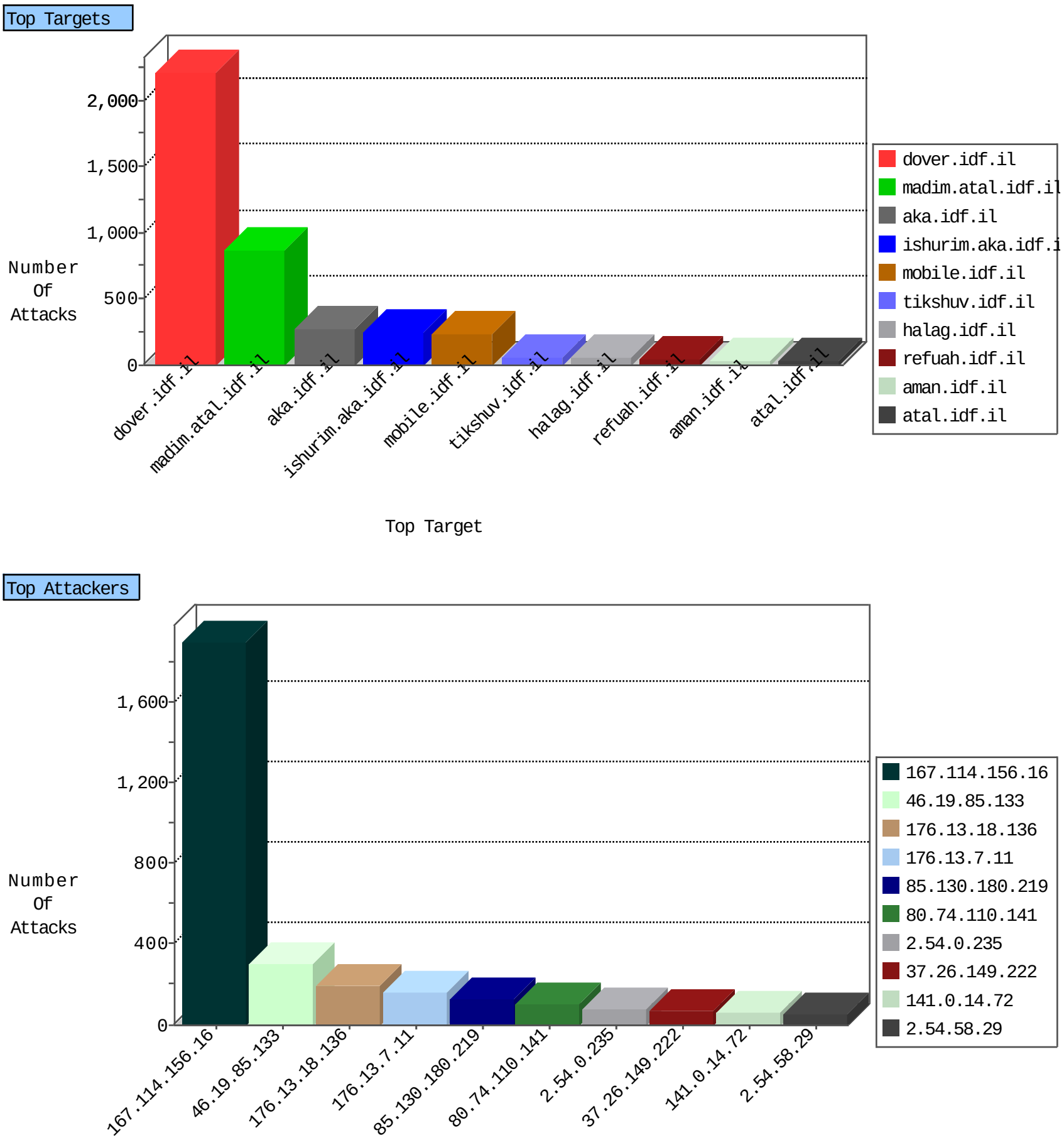
01-07-2016-10:04:00 to 01-07-2016-11:04:00

IDF Under Attack Daily Report



01-07-2016-10:04:00 to 01-07-2016-11:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.73.214	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	6696
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3905
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3337
82.81.12.22	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
223.4.174.30	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
77.247.178.132	Netherlands	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

01-07-2016-10:04:00 to 01-07-2016-11:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.207		147.237.76.200	eitan.aka.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
185.130.5.207		147.237.76.200	eitan.aka.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

01-07-2016-10:04:00 to 01-07-2016-11:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.0.235	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	32
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.78.67	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
197.211.229.238	147.237.77.74	Zimbabwe	law.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.207	147.237.76.42		refuah.idf.il	ET WEB_SERVER Muieblackcat scanner	1
173.199.74.136	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.64.240.28	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.99.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.194.206.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
197.211.229.238	147.237.77.74	Zimbabwe	law.idf.il	ET SCAN NMAP -sS window 4096	1
176.13.0.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
173.199.74.136	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.226.20.85	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
223.4.174.30	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.179.155.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-07-2016-10:04:00 to 01-07-2016-11:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.130.180.219	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
37.26.149.222	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
141.0.14.72	Europe	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	60
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
2.54.0.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
2.52.186.202	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
62.219.99.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
176.13.12.123	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
80.246.133.5	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
176.13.19.94	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.20.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.153	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.20.10	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.133.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.66.103.114	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
185.120.126.102		147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.110.33	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
37.26.148.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.33.11	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
91.135.102.174	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
168.168.43.250	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.8	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
103.18.75.48	India	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
185.120.125.25		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.117.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
103.18.75.48	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.127.184.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.218.231	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	6
199.203.63.34	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.13.184	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.228.129	Israel	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	6
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.67.32.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.192	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
85.64.130.142	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.0.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.0.235	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Urgent Data Enforcement	TCP segment with urgent pointer (no data). Urgent data indication was stripped. Please refer to sk36869.	alert	5
46.19.85.157	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.0.235	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Urgent Data Enforcement	TCP segment with urgent pointer (no data). Urgent data indication was stripped. Please refer to sk36869.	drop	5
109.64.139.144	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.110	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.39.173	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.64.130.142	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.0.235	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.26.146.151	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

01-07-2016-10:04:00 to 01-07-2016-11:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	163
176.13.18.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
46.19.85.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
176.13.7.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
80.74.110.141	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many of the Same Response Code (404) in Session from 80.74.110.141	Block	100
176.13.18.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	66
176.13.7.11	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.7.11	Block	52
2.54.58.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
109.253.212.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
2.54.62.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
46.19.85.133	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.133	Block	22
176.13.23.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
46.19.86.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
37.26.149.222	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
62.219.99.130	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
46.19.86.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.86.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.13.18.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	5
176.13.12.123	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.13.19.94	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.13.20.10	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.13.21.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.54.133.224	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.142.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.204.64	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	3
109.253.137.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	3
2.54.184.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.204.64	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.8.204.64	Block	3
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	3
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	3
109.253.137.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.193.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.120.126.102		147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
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	2
2.52.5.84	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
46.19.86.140	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
212.235.98.139	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 212.235.98.139	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
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
46.19.85.153	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
109.253.131.131	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	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	1
62.219.170.25	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/sachar/login/	Block	1
2.54.166.229	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 2.54.166.229	Block	1

01-07-2016-10:04:00 to 01-07-2016-11:04:00