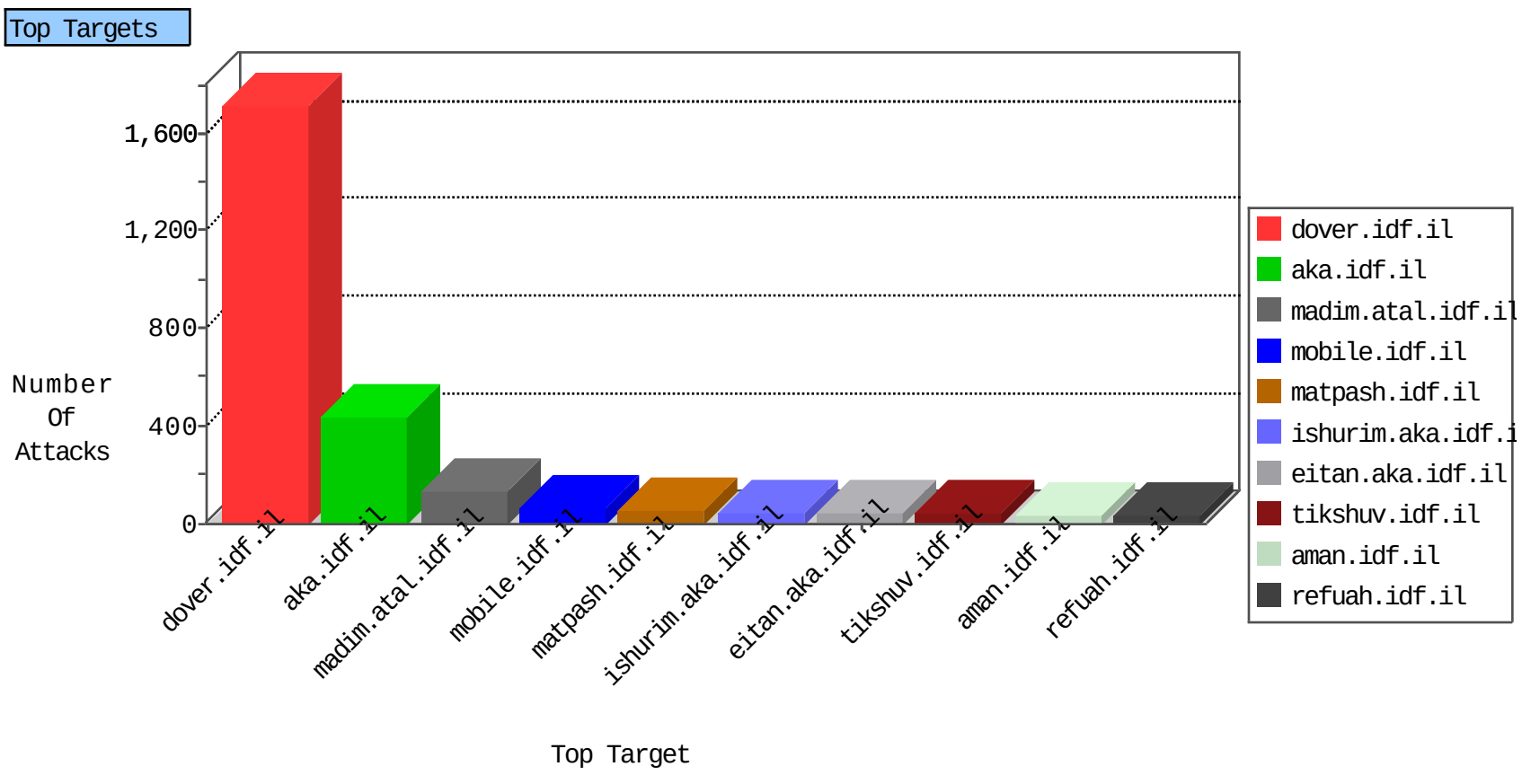
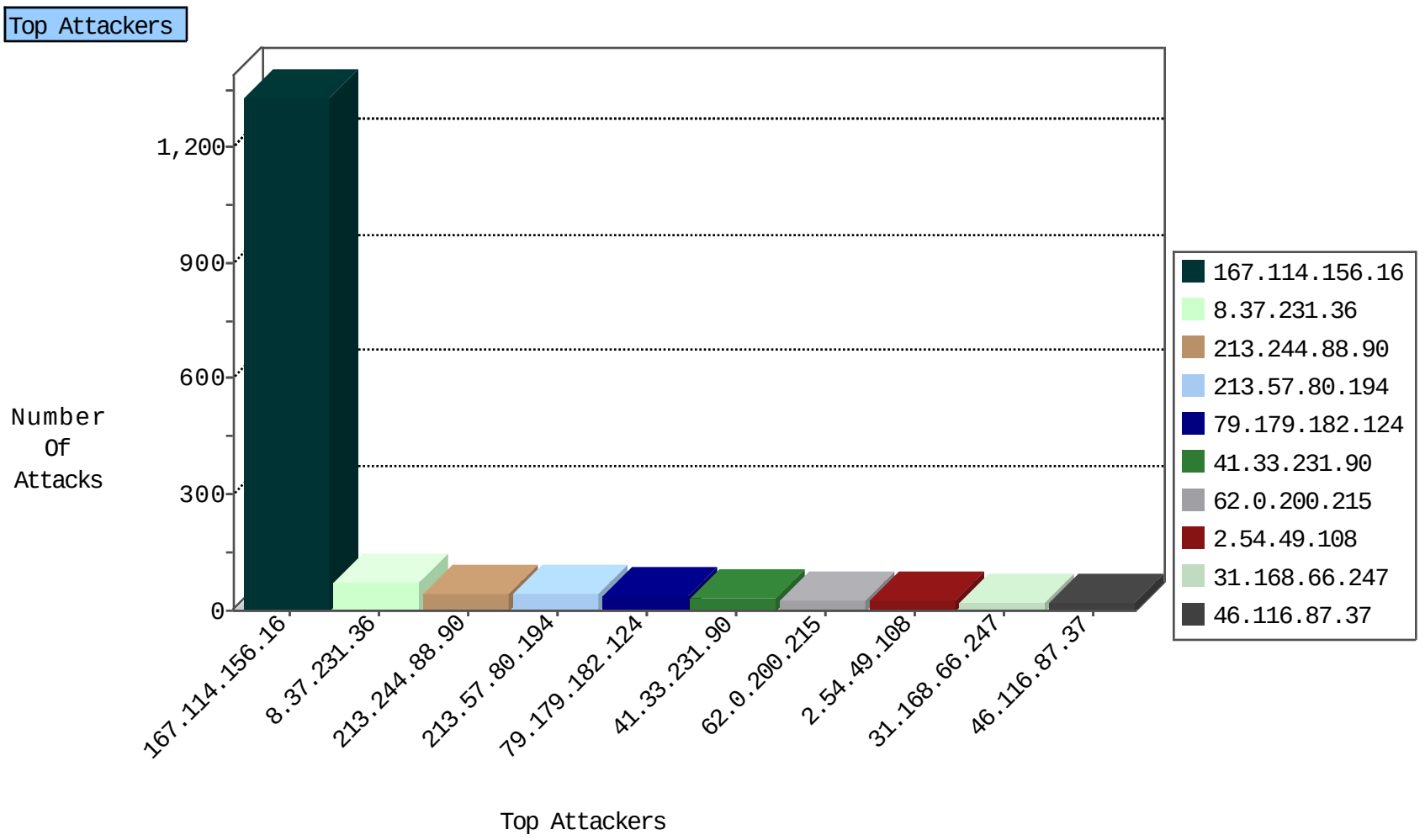
01-07-2016-13:04:07 to 01-07-2016-14:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-07-2016-13:04:07 to 01-07-2016-14:04:07

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	3056
8.37.70.90	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
80.246.130.220	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
8.37.231.36	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
146.185.239.100	Russian Federation	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
77.247.178.132	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

01-07-2016-13:04:07 to 01-07-2016-14:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
222.84.7.163	China	147.237.76.31	nakchal.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	3
66.240.213.93	United States	147.237.76.176	test.ncore.idf.i	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1

01-07-2016-13:04:07 to 01-07-2016-14:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.178.196.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.73.206	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
59.45.79.117	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 2048	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
183.61.109.189	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
46.19.86.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.160.131.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.11.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.182.115.118	147.237.77.216	Belgium	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.105.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.63.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.69	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	1
59.45.79.117	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
197.211.229.238	147.237.8.27	Zimbabwe	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
58.253.96.122	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -f -sS	1
193.105.134.220	147.237.77.179	Sweden	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.61.109.189	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
41.33.29.71	147.237.77.243	Egypt	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
95.86.94.7	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.41.203	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.50.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-07-2016-13:04:07 to 01-07-2016-14:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.231.36	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	70
213.57.80.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
213.244.88.90	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
62.0.200.215	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
46.19.85.140	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	21
79.179.182.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
207.241.229.192	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
79.179.182.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
2.52.154.188	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
109.253.222.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
65.49.14.73	Anonymous Proxy	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
46.116.87.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
176.13.17.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.116.87.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	10
132.64.25.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
43.255.176.89	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.115.83.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.26.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.125.15		147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.11.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.36.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.161	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.1.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.174	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.66.124.56	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.154	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.174	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.17.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.249.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.210.137.25	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.115.83.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.149.235	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.67.17.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.183.70	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.125.15		147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.11.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.123	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
176.13.15.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
2.54.46.91	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

01-07-2016-13:04:07 to 01-07-2016-14:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.49.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
31.168.66.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
2.54.58.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
109.253.131.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
217.194.202.110	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 217.194.202.110	Block	15
2.54.4.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
195.95.183.254	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 195.95.183.254	Block	8
2.54.167.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.21.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.9	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
80.246.137.196	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	5
80.246.140.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	4
79.181.162.57	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	4
185.32.179.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.70.243	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	3
109.253.222.201	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	3
2.54.183.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.17.12	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.11.101	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/resource/userfollowresource/create/	Block	3
79.181.162.57	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19783-he/idfgdover.aspx/	Block	2
159.203.82.47	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 159.203.82.47	Block	2
46.19.85.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.179.182.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.131.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
103.255.6.94	Pakistan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	2
2.52.152.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.133.75	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtID in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
2.54.44.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.123	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/includes/codegen/cms_codegen.php	Block	1
5.22.131.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.48.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.196.174	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
50.62.176.72	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
87.69.170.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.4.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.64	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	1
109.253.217.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.146.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.186.190.195	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
2.54.163.98	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.86.70.243	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9234-he/refuah.aspx	Block	1
195.95.183.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
2.54.30.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.111.9.100	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.116.87.37	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 46.116.87.37	Block	1
109.253.136.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-07-2016-13:04:07 to 01-07-2016-14:04:07