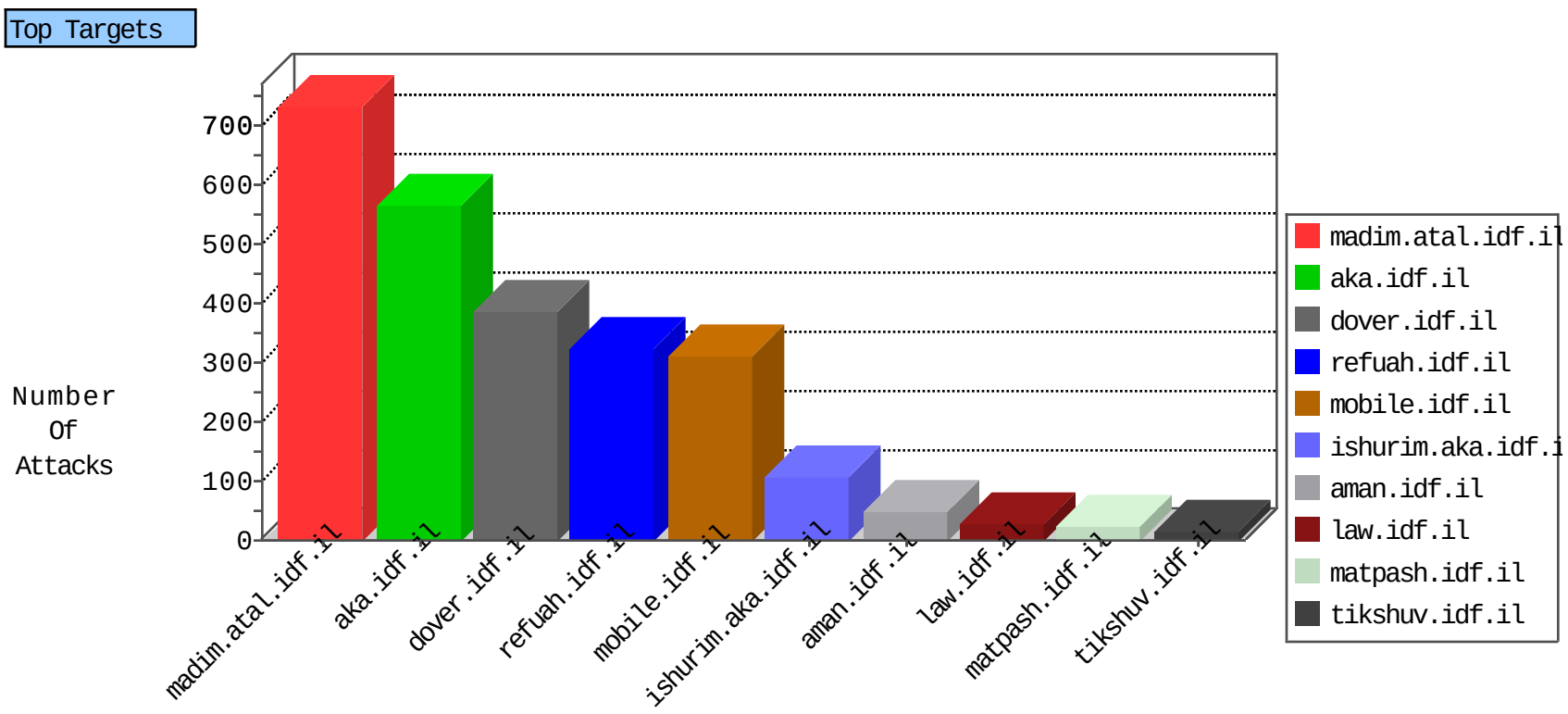
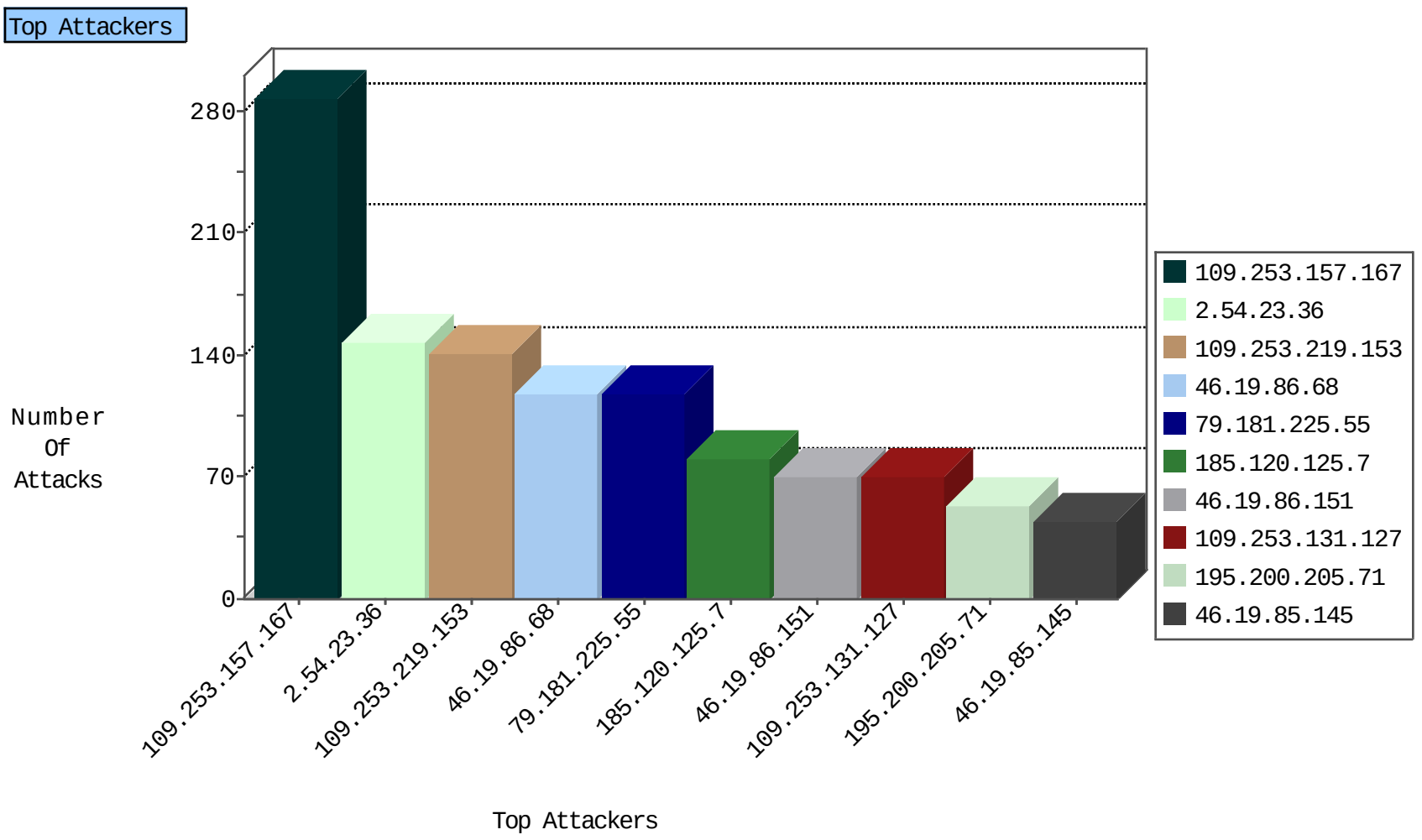
02-01-2016-12:04:01 to 02-01-2016-13:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-01-2016-12:04:01 to 02-01-2016-13:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	18
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	6
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
89.248.174.4	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
89.248.174.4	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

02-01-2016-12:04:01 to 02-01-2016-13:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-01-2016-12:04:01 to 02-01-2016-13:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.26.146.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.151.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.144.62.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.145.181	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.76.202	Sweden	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
146.0.75.114	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
94.76.3.122	147.237.72.166	Bahrain	aka.idf.il	ET SCAN NMAP -sS window 1024	1
51.255.127.25	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
82.80.193.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.238.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.4.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.184.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.169.207	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
59.45.79.117	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
185.120.125.27	147.237.72.166		aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
109.66.162.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
84.109.165.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
51.255.127.25	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
80.246.136.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-01-2016-12:04:01 to 02-01-2016-13:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.181.225.55	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	118
46.19.86.151	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	57
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	54
109.253.131.127	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
77.127.148.5	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
62.0.197.105	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	33
2.54.175.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
195.200.205.71	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	27
195.200.205.71	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	26
2.54.10.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.210.54.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
2.52.138.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.86.68	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
93.172.241.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.173	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
37.26.148.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.219.59	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.178.252	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.136.80	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.68	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.183	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
31.223.191.205	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.253.158.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.147.230	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.151	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.173.227	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.252	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.164	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.68	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.86.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.85.145	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
5.29.3.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
5.29.3.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.6.123	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.183.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.235.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.145.220.112	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.179.5.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.68	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.245.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.134.60	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.8.240	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.183.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6

02-01-2016-12:04:01 to 02-01-2016-13:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.157.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	150
109.253.219.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	141
109.253.157.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	120
2.54.23.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	95
2.54.23.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	53
46.19.85.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
46.19.85.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
46.19.85.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
109.253.157.167	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 109.253.157.167	Block	17
109.253.131.127	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	16
109.253.221.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
109.253.139.146	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	14
2.54.151.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
79.176.240.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
176.97.116.135	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
2.54.177.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
93.172.241.126	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
2.54.10.14	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.97.116.135	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.97.116.135	Block	5
46.210.54.253	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.52.138.20	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.54.178.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
76.115.96.90	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.147.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
80.246.140.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.139.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.228.5.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.136.80	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.4.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.148.241	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.151	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.158.16	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
192.116.55.253	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
212.179.40.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
132.70.226.206	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	1
46.19.85.44	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
109.253.192.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.180.237.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
191.232.136.163	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
31.168.227.138	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl61 in www.aka.idf.il/main/sachar/payslips.aspx	None	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
176.97.116.135	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Malformed URL [[#28]][[#21]]×›×ªjj	Block	1
91.200.12.136	Ukraine	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/0/2910.pdf#search=	Block	1
192.118.36.53	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/71663.pdf	Block	1
46.19.85.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.215.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

02-01-2016-12:04:01 to 02-01-2016-13:04:01