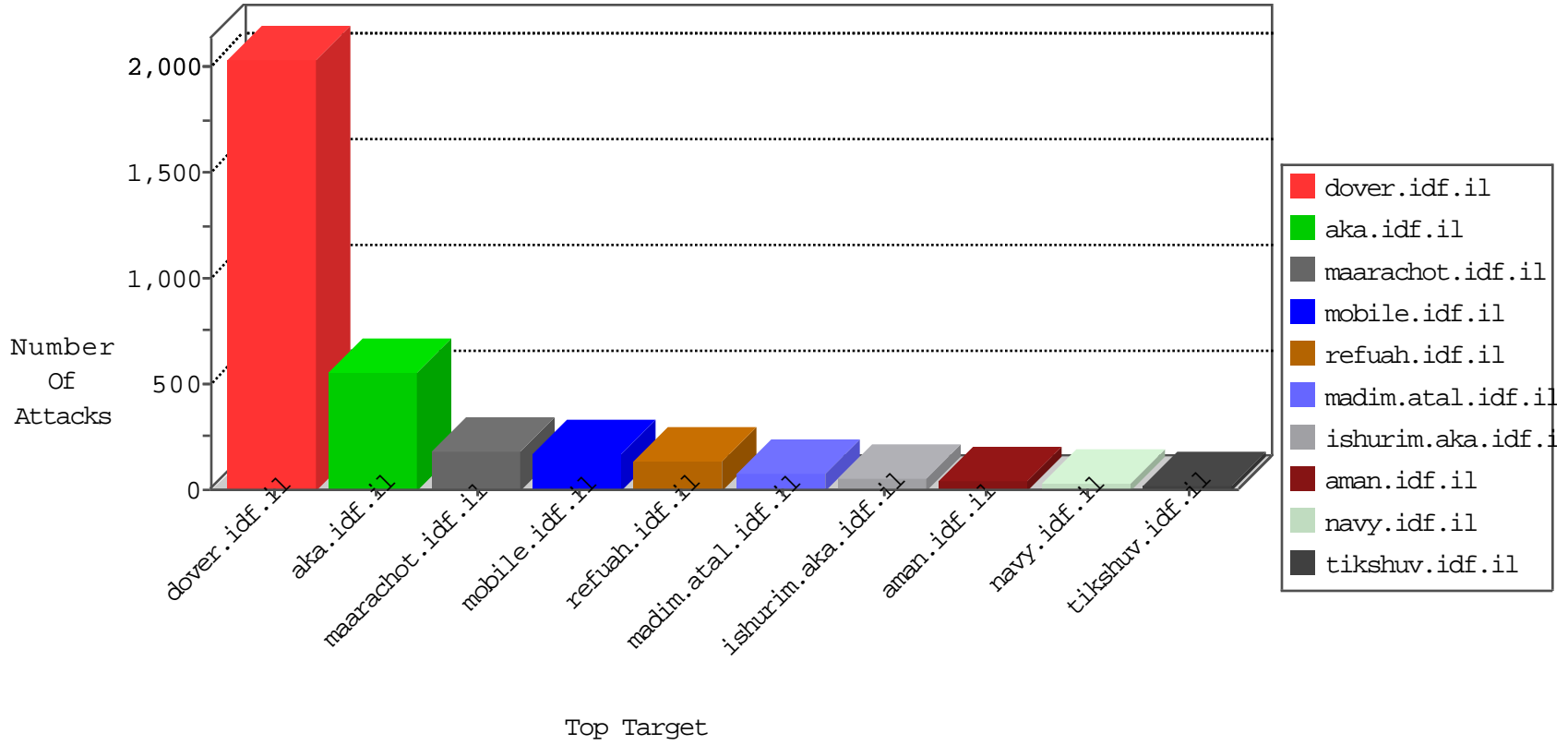


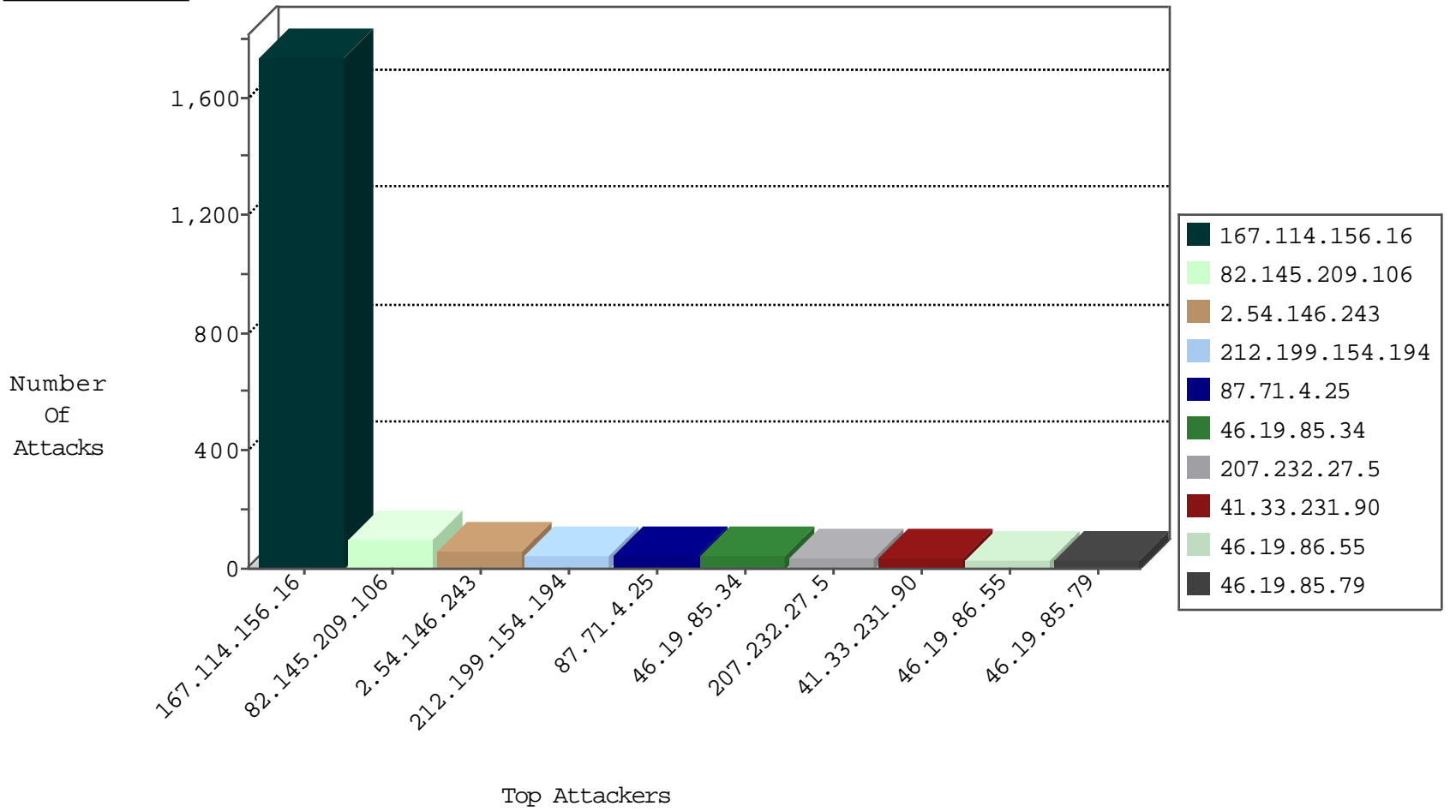
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3069
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	251
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
82.145.209.106	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	95
81.218.146.238	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
31.168.133.226	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
198.20.69.98	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
116.26.30.139	China	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

01-03-2016-10:04:06 to 01-03-2016-11:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
198.20.69.98	147.237.77.227	United States	e.hamaz.idf.il	ET DROP Dshield Block Listed Source	1
185.130.5.224	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.207	147.237.77.61		e.cogat.idf.il	ET SCAN Potential SSH Scan	1
89.138.118.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
46.121.90.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.31.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.231	147.237.76.148		ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.207	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.207	147.237.76.202		e.halag.idf.il	ET SCAN Potential SSH Scan	1
82.80.135.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.131.174	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.71.4.25	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	43
207.232.27.5	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
46.19.85.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
46.19.85.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
212.199.154.194	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
2.54.146.243	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
46.19.85.232	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.64.66.235	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
77.126.88.191	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.173.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
79.182.212.134	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
84.228.163.243	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
46.19.85.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.160.151.25	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.13.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
62.0.229.129	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	11
2.54.146.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.146.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
2.54.146.243	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	10
2.54.146.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
79.178.170.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.179.28.34	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
82.166.137.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.147.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.2.43	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
62.0.67.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.64.164.21	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
105.196.255.70	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
62.219.114.144	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
176.13.4.25	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
213.140.59.140	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.114.91.248	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
98.210.169.38	United States	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
217.194.207.24	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.29	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.147.217	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.103.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.196.44	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.55	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.7.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.29	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.12.137.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
105.196.255.70	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.22.146	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	12
87.69.39.95	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.39.95	Block	11
46.19.85.34	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
109.253.208.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.184.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.65.43.7	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	5
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	5
37.26.148.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.54.25.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.156.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
37.26.146.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.200.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.232	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.180	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	4
195.200.205.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/8/	Block	3
2.54.3.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.143.112.217	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	2
2.54.60.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.221.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.157	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
176.12.137.165	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.179.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
5.28.177.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.177.112.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.3.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.60.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.117.156.160	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
109.253.130.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.69.39.95	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.69.39.95	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
46.19.85.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.139.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.22.146	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
176.12.144.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.138.67.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.179	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
212.179.159.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
46.210.136.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.160.151.25	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.12.144.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.81.193.82	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1119-he/nakhal.aspx	Block	2
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	2
79.181.181.213	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.181.181.213	Block	2