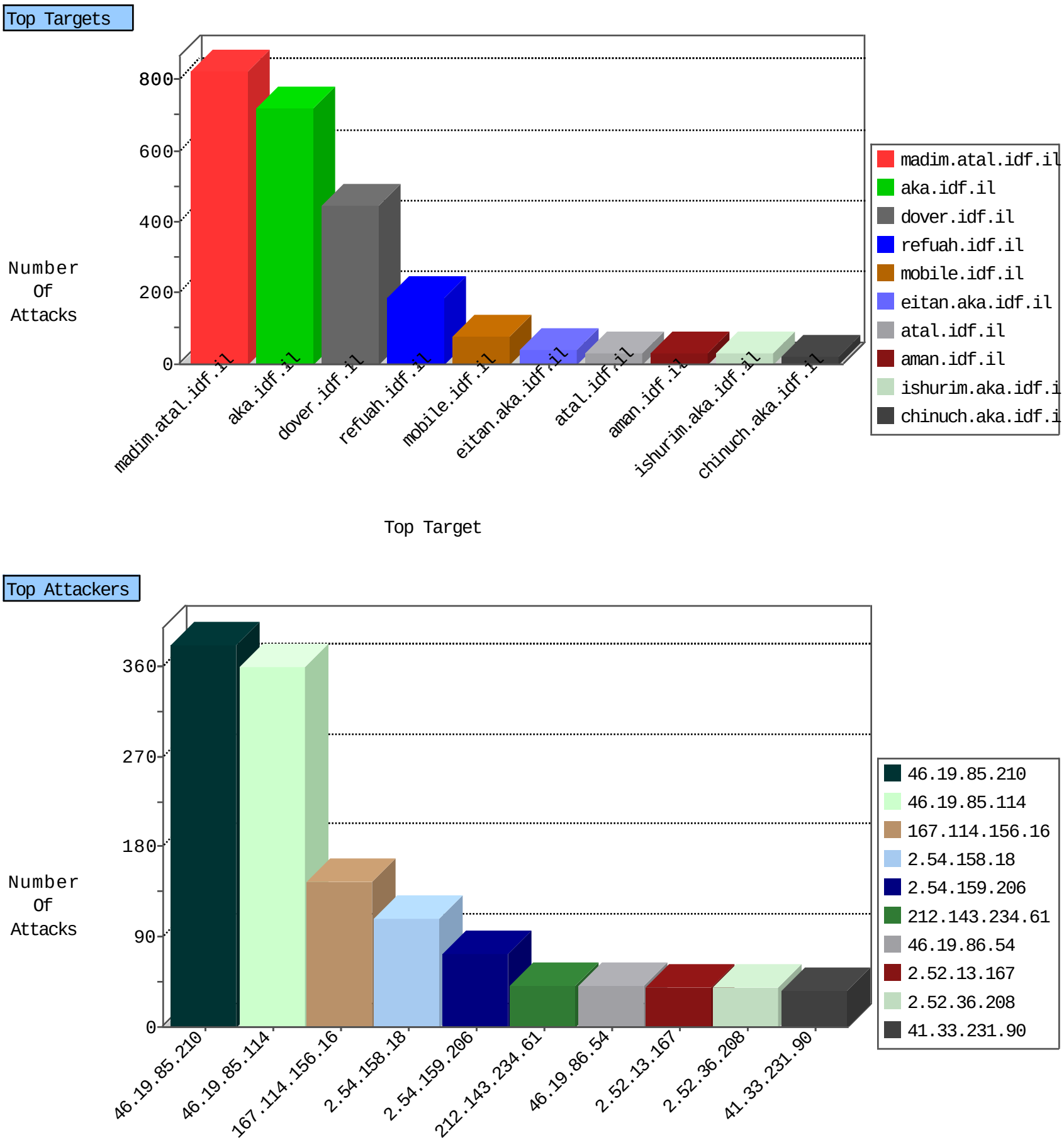
12-29-2015-09:04:01 to 12-29-2015-10:04:01

IDF Under Attack Daily Report



12-29-2015-09:04:01 to 12-29-2015-10:04:01

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	3398
79.179.48.62	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	5
157.55.39.237	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
119.138.128.207	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
151.217.178.35		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
185.106.92.173		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
119.138.128.207	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.106.92.173		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
119.138.128.207	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
77.247.178.132	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

12-29-2015-09:04:01 to 12-29-2015-10:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-29-2015-09:04:01 to 12-29-2015-10:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
193.104.41.54	147.237.76.198	Moldova, Republic of	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
31.168.170.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.39.222.253	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
182.74.68.35	147.237.77.226	India	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
182.74.68.35	147.237.77.176	India	matpash.idf.il	ET SCAN Potential SSH Scan	1
132.65.125.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.233.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
63.141.217.229	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.8.27	Cote D'Ivoire	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
37.26.147.225	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.104.41.54	147.237.76.86	Moldova, Republic of	navy.idf.il	ET SCAN Potential SSH Scan	1
31.168.24.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
182.74.68.35	147.237.77.234	India	halag.idf.il	ET SCAN Potential SSH Scan	1
2.54.27.101	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
182.74.68.35	147.237.77.205	India	prisha.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.8.14		e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.114	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
80.179.40.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.120.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-29-2015-09:04:01 to 12-29-2015-10:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.158.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
79.177.132.122	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
185.38.14.215	Netherlands	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
2.54.159.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
212.143.234.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
185.89.217.234		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
46.19.86.109	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.253.199.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	17
2.54.159.206	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	17
2.54.158.18	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	16
46.120.5.59	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
115.79.46.50	Vietnam	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
185.89.217.231		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
185.89.217.227		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	14
2.54.158.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
2.54.158.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	14
185.89.217.233		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	13
2.54.158.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
2.54.159.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.120.123.149	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.159.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
2.54.159.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.120.74.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.120.5.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	11
2.52.13.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
212.143.234.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
185.89.217.226		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
2.52.36.208	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	10
2.54.158.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.67.51.57	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.86.45	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.52.36.208	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
147.236.238.41	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
2.52.13.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.23.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
2.52.13.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
46.120.74.230	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
149.78.231.119	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	8
185.89.217.235		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
2.52.13.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
62.0.200.211	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.126	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.36.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
37.26.147.174	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
2.52.36.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
185.89.217.224		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7

12-29-2015-09:04:01 to 12-29-2015-10:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	187
46.19.85.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	179
46.19.85.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	160
46.19.85.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.85.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	94
46.19.86.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
185.32.179.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.85.114	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.114	Block	13
66.249.66.28	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	9
46.19.86.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
109.253.199.158	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
80.179.115.198	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 80.179.115.198	Block	4
46.19.85.204	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.19.86.109	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
85.93.91.84	Germany	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
217.194.203.52	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
118.173.208.149	Thailand	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.64.119.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.131.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.142.189.251	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/4/size338x0/1584.jpg	Block	2
176.13.11.125	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
46.19.86.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.131.29	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/1133-22638-he/dover.aspx.	Block	2
72.47.228.27	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
180.30.222.11	Japan	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/general/	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
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
149.50.92.9	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.149.221	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
2.54.129.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.aspx.	Block	1
46.19.86.130	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
109.253.132.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.185.124	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.176.204.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.89.217.235		147.237.76.42	refuah.idf.il	URL is Above Root Directory www.refua.atal.idf.il/../images/shared/home.png	Block	1
46.19.85.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.139.159.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.46	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
176.13.8.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.0.111.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.156.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.137.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.181.54	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
2.52.41.170	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
79.181.32.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.125.112.10	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.125.112.10	Block	1
180.76.15.15	China	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	1

12-29-2015-09:04:01 to 12-29-2015-10:04:01