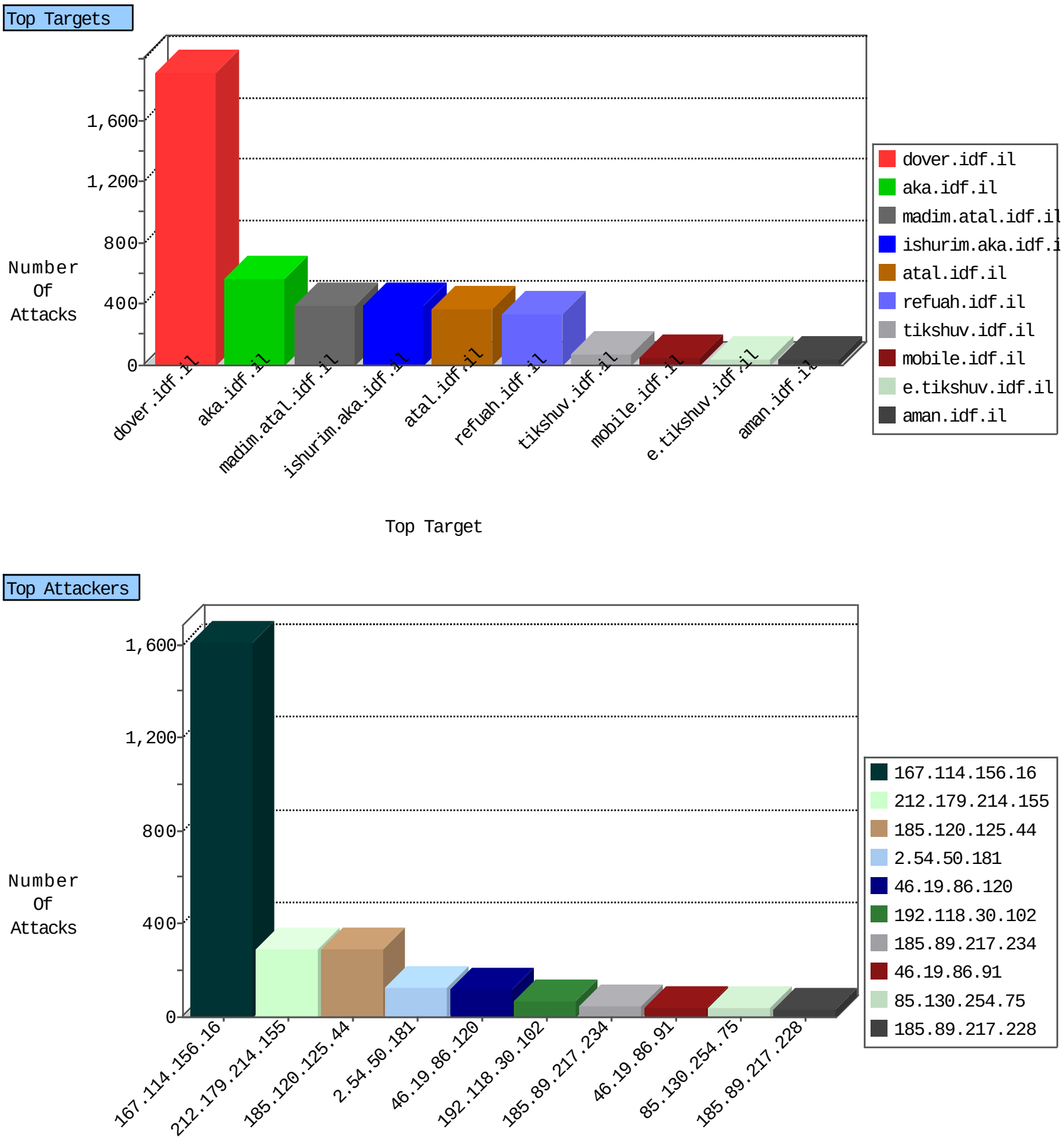
01-14-2016-13:04:09 to 01-14-2016-14:04:09

IDF Under Attack Daily Report



01-14-2016-13:04:09 to 01-14-2016-14:04:09

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	3050
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	779
212.235.98.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
212.150.82.114	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
222.174.5.14	China	147.237.0.35	akaws.idf.il	Frk_Under_Attack_Con_Tcp	drop	2

01-14-2016-13:04:09 to 01-14-2016-14:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-14-2016-13:04:09 to 01-14-2016-14:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
193.105.134.220	147.237.76.177	Sweden	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
113.171.23.126	147.237.77.74	Vietnam	law.idf.il	ET SCAN Potential SSH Scan	1
109.251.56.171	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.60.153.178	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.141.195	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.76.148	Sweden	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.147.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.138.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.134.208	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.253.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-14-2016-13:04:09 to 01-14-2016-14:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.214.155	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	282
185.120.125.44		147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	268
46.19.86.91	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
185.130.5.207		147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	30
185.89.217.234		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	26
185.89.217.231		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	25
185.89.217.228		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	25
185.89.217.230		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	22
46.19.86.132	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
185.89.217.234		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	21
185.89.217.226		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
185.89.217.229		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
185.89.217.233		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
185.89.217.235		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	16
69.64.48.162	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	15
2.54.12.248	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
185.89.217.225		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
185.89.217.232		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
185.89.217.224		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
185.120.125.44		147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
185.89.217.235		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	14
85.130.254.75	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
185.89.217.227		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	13
68.64.167.142	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	13
185.89.217.233		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	12
31.210.176.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.34	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
31.210.176.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
69.60.111.84	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	12
2.52.191.250	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.111	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
185.120.125.44		147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
85.130.254.75	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
2.52.191.250	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
185.89.217.228		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	10
185.89.217.226		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	10
85.130.254.75	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	10
185.89.217.229		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	10
109.253.128.206	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.88	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
17.78.79.134	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.186.23.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.150.82.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.149.129	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.42.109	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.13.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	81
2.54.50.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	80
2.54.50.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	46
46.19.86.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	33
2.54.62.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
2.54.20.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
37.26.149.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
2.54.50.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
84.109.154.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
109.253.130.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
5.175.13.138	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.175.13.138	Block	3
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.149.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.178.209.4	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 79.178.209.4	Block	3
95.86.103.110	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	2
2.54.42.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.178.225.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.178.225.227	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
176.13.19.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.176.105.13	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.176.105.13	Block	2
62.176.112.77	Bulgaria	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.120.125.44		147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
5.29.237.174	Israel	147.237.77.234	halag.idf.il	Parameter Type Violation search in www.logistics.atal.idf.il/1213-he/halag.aspx	Block	1
94.242.246.23	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
82.213.48.122	Palestinian Territory, Occupied	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
167.114.119.241	Canada	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
79.181.111.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.45	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.135.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.148.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
68.180.231.40	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/youtu.be/dsh2chqxxt0	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
85.250.246.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.3.144.87	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
46.19.85.185	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
128.73.83.250	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
80.246.138.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.105.13	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/sachar	Block	1
37.26.149.255	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.65.118.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
193.143.77.10	Poland	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
95.86.103.110	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.86.103.110	Block	1
84.108.219.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.0.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.186.230	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/×'×™××•×¡	Block	1
109.253.139.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1