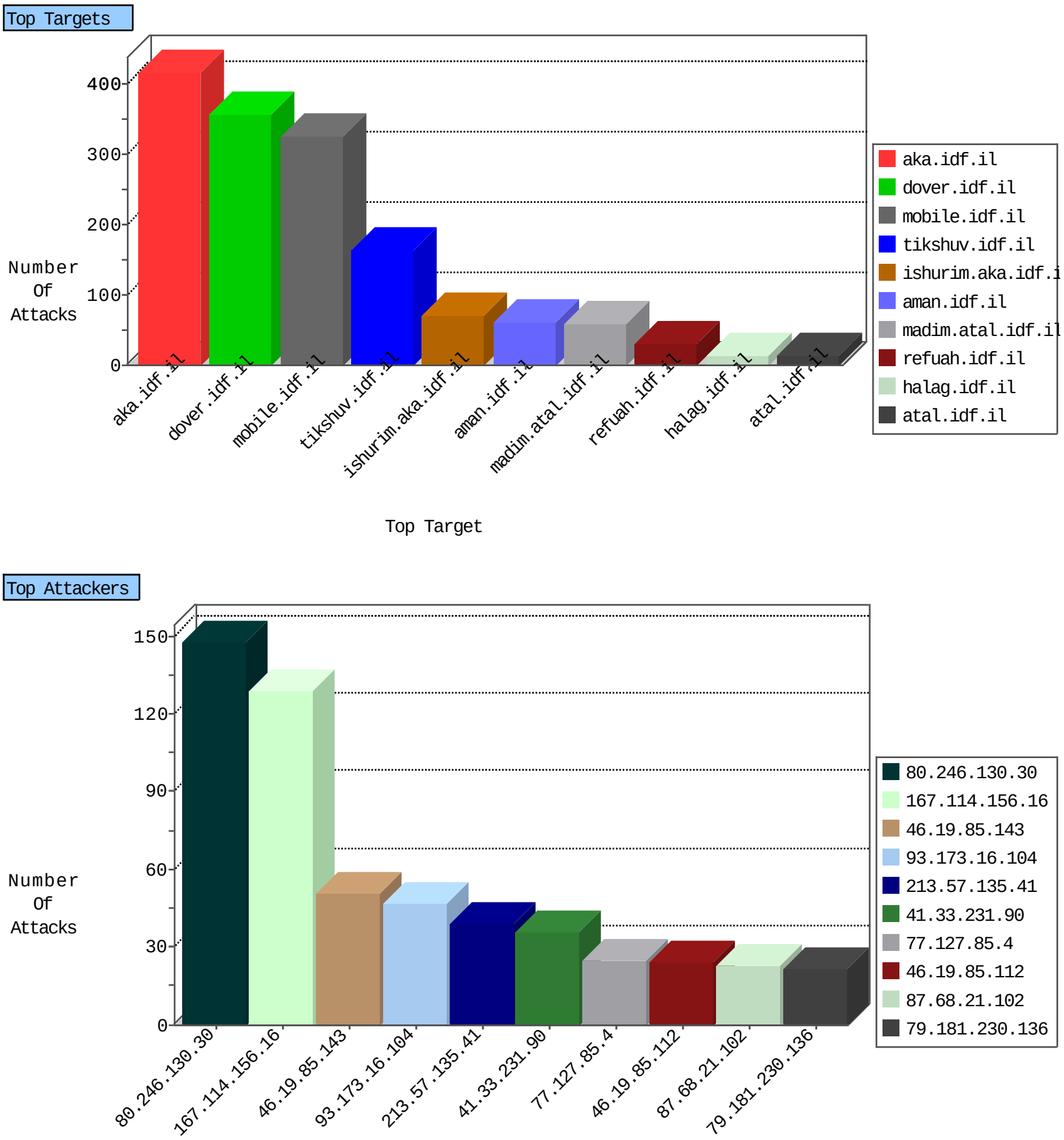
12-29-2015-20:04:07 to 12-29-2015-21:04:07

IDF Under Attack Daily Report



12-29-2015-20:04:07 to 12-29-2015-21:04:07

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	3700
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1634
66.249.78.9	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	652
66.249.64.243	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
172.98.67.124		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
79.158.138.247	Spain	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
40.77.167.77	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

12-29-2015-20:04:07 to 12-29-2015-21:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-29-2015-20:04:07 to 12-29-2015-21:04:07

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	4
50.204.188.142	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 2048	1
151.217.178.88	147.237.76.196		e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.151.52.195	147.237.76.30	Ukraine	himush.idf.il	ET SCAN NMAP -sS window 1024	1
202.59.169.38	147.237.77.235	Indonesia	sviva.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.55	147.237.77.205		prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.59.169.38	147.237.77.227	Indonesia	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.55	147.237.77.19		law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.59.169.38	147.237.77.216	Indonesia	dover.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.55	147.237.76.177		ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.59.169.38	147.237.77.178	Indonesia	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.55	147.237.8.14		e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.59.169.38	147.237.77.170	Indonesia	maarachot.idf.il	ET SCAN Potential SSH Scan	1
139.91.210.41	147.237.76.44	Greece	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
202.59.169.38	147.237.77.74	Indonesia	law.idf.il	ET SCAN Potential SSH Scan	1
79.181.204.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
201.173.163.44	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
50.204.188.142	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 3072	1
185.32.179.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
50.204.188.142	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -f -sS	1
202.59.169.38	147.237.77.243	Indonesia	mobile.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.76.148		gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.59.169.38	147.237.77.234	Indonesia	halag.idf.il	ET SCAN Potential SSH Scan	1
5.220.50.133	147.237.77.170	Iran, Islamic Republic of	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
151.217.178.55	147.237.77.178		e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.59.169.38	147.237.77.226	Indonesia	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.55	147.237.76.197		e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.59.169.38	147.237.77.212	Indonesia	e.dover.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.55	147.237.76.86		navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.59.169.38	147.237.77.176	Indonesia	matpash.idf.il	ET SCAN Potential SSH Scan	1
149.78.180.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
202.59.169.38	147.237.77.121	Indonesia	e.navy.idf.il	ET SCAN Potential SSH Scan	1
104.143.14.247	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
202.59.169.38	147.237.77.61	Indonesia	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
77.127.165.69	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-29-2015-20:04:07 to 12-29-2015-21:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.173.16.104	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
46.19.85.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
213.57.135.41	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.86.50	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	20
46.19.85.112	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
79.181.230.136	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.149.225	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
77.127.239.13	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
176.13.18.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
85.250.249.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
66.249.66.63	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.88.126.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.127.85.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.66.36.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.4	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.86.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.102.254.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
87.69.20.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.186	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
82.142.109.74	Czech Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.151.174	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.211.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.159.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.129.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.225	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.154.17	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
88.27.64.202	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
37.26.147.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.28.169.76	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.184.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.21.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.112	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.122.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.233.119	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.148.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.174.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.160.206.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.104.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
84.228.19.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

12-29-2015-20:04:07 to 12-29-2015-21:04:07

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.129.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.187.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.198.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.130.30	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	148
46.19.86.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
213.8.204.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
46.19.85.143	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	12
77.127.85.4	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 77.127.85.4	Block	9
132.66.223.59	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 132.66.223.59	Block	9
93.173.16.104	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
109.64.160.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
79.181.230.136	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.13.8.89	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	4
176.13.10.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
24.0.111.135	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 24.0.111.135	Block	3
85.250.214.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.88.126.44	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.176.108.254	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
95.86.71.207	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 95.86.71.207	Block	3
85.250.249.93	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.18.134	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
87.69.20.81	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
77.127.85.4	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
37.142.184.152	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.67.21.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.13.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.152	Israel	147.237.77.243	mobile.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
41.230.14.223	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	2
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	2
77.127.85.4	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.8.89	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
31.154.145.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.139	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.225	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.147	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/activity-log/create	Block	2
46.19.85.138	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
95.86.82.166	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1217-he/refuah.aspx&sa=u&ved=0ahukewjwxt6e14hkahxd7w4khuwpakgqfggimaa&usg=afqjcnfizknidff3fqlewsd0woh6p4ybbg	Block	2
157.55.39.178	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.54.37.29	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
94.159.225.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.168.121.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.59.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.76	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/mobile/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
149.88.125.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.7.165	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
79.183.214.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.179.42.225	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
46.116.128.8	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1