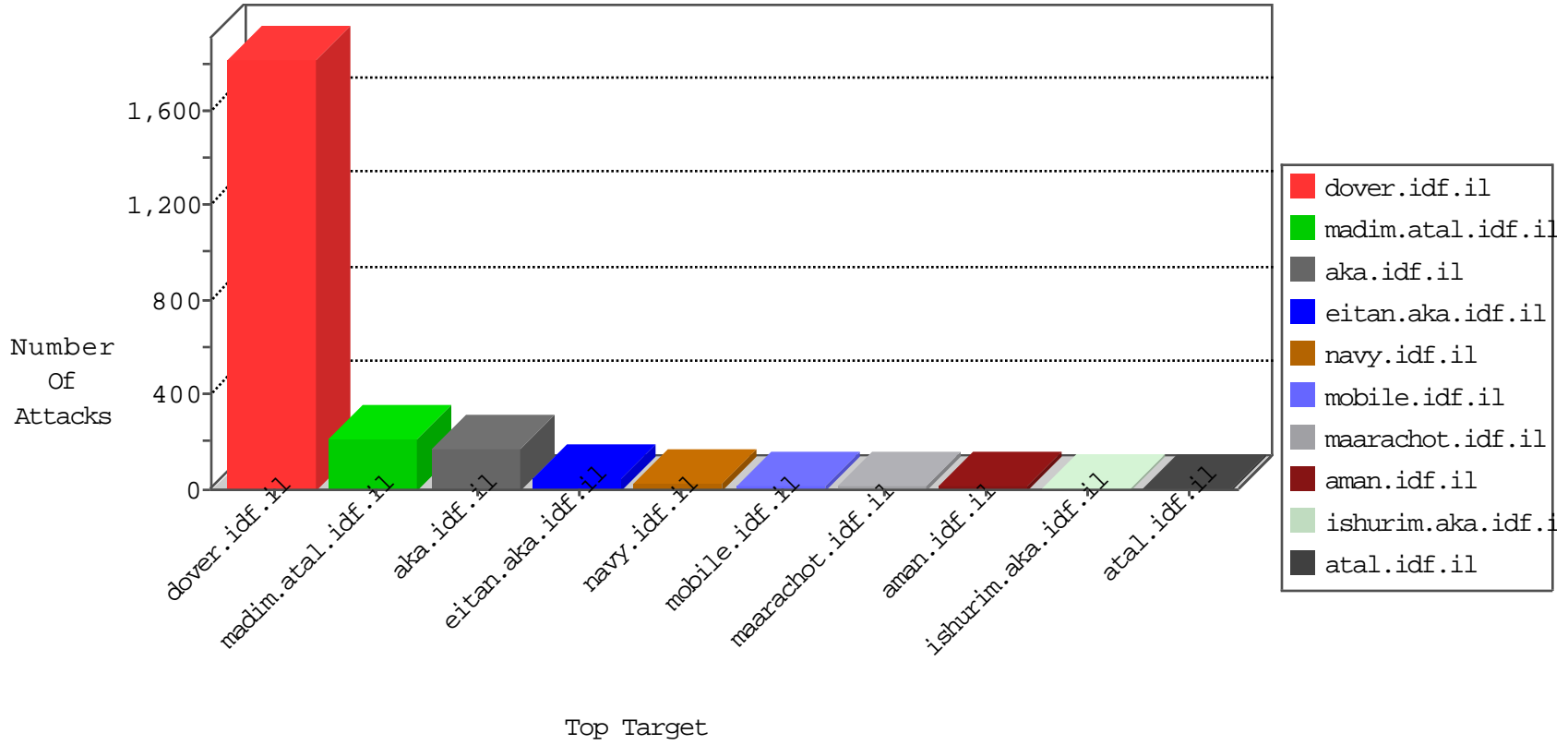


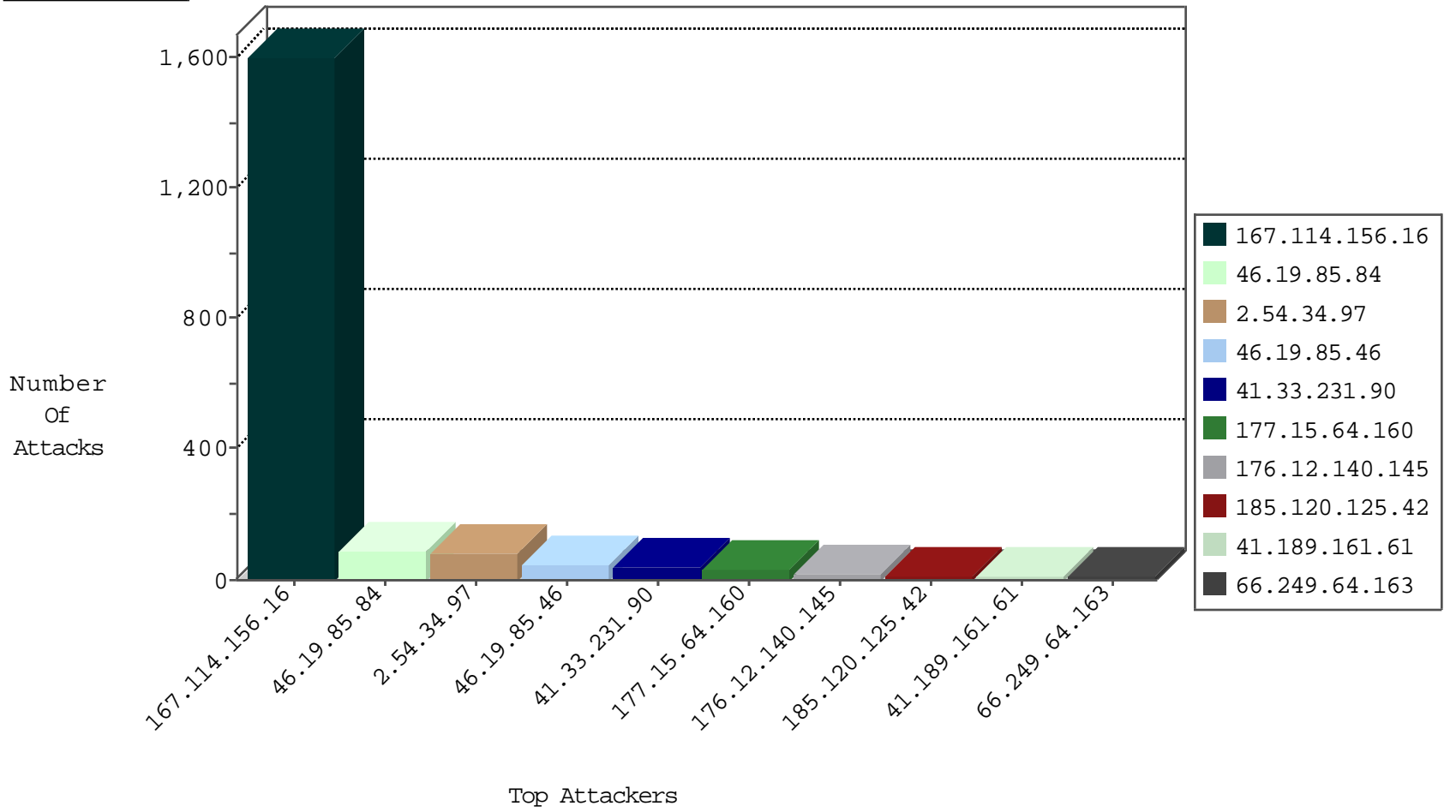
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3868
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3642
66.249.78.160	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	218
185.120.125.42		147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	11
109.66.204.68	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
94.102.56.238	Netherlands	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1

12-23-2015-21:04:02 to 12-23-2015-22:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.147	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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
5.39.222.253	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
220.189.157.89	147.237.76.34	China	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.39.222.253	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
189.197.250.120	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.164.7.249	147.237.77.243	Vietnam	mobile.idf.il	ET SCAN Potential SSH Scan	1
113.164.7.249	147.237.77.205	Vietnam	prisha.idf.il	ET SCAN Potential SSH Scan	1
113.164.7.249	147.237.77.170	Vietnam	maarachot.idf.il	ET SCAN Potential SSH Scan	1
113.164.7.249	147.237.77.74	Vietnam	law.idf.il	ET SCAN Potential SSH Scan	1
84.228.70.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.224.78.176	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.164.7.249	147.237.77.212	Vietnam	e.dover.idf.il	ET SCAN Potential SSH Scan	1
113.164.7.249	147.237.77.179	Vietnam	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
113.164.7.249	147.237.77.121	Vietnam	e.navy.idf.il	ET SCAN Potential SSH Scan	1
113.164.7.249	147.237.77.61	Vietnam	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
62.75.236.76	147.237.0.34	Germany	tikshuv.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
46.19.85.46	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
177.15.64.160	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.189.161.61	Ghana	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.28.176.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.66.144.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.164	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.160.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.0.81.17	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.52.22.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.176.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.144.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.147.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.114	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
31.210.186.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.33	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.12.140.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.241	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
128.78.78.156	France	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.67.59.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.96.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.175.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.112.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.169.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.188.29.98	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.46.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.42		147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
37.26.148.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
5.29.179.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
5.102.254.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
213.57.129.222	Israel	147.237.72.156	anan.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.179.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.149.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
85.250.223.57	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.25.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.106.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.160	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.64.169	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
213.57.135.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2

12-23-2015-21:04:02 to 12-23-2015-22:04:02

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.11	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.241	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
2.54.34.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
176.12.140.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
37.142.191.36	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	9
84.94.22.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
85.250.223.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.145.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.25.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.213.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.23.188	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
158.69.52.102	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
31.215.24.208	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	2
2.52.47.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.142.142.49	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	2
149.78.68.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.142.178.40	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
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
85.250.223.57	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1540	Block	2
79.183.187.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.215.24.208	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
79.183.211.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.230.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.64.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.221.23	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.34.97	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.34.97	Block	1
109.64.176.21	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1756	Block	1
194.150.168.95	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.108.172.133	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.120.255.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.191.36	Israel	147.237.72.166	aka.idf.il	Unknown Parameter _ in www.aka.idf.il/main/giyus/general.aspx	None	1
79.182.216.192	Israel	147.237.72.166	aka.idf.il	Illegal Parameter Encoding ct100\$ct100h in www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	None	1
79.176.129.21	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.201.154.241	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.73.146	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19915-he/dover.aspx	Block	1
212.143.76.93	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
93.173.128.203	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
80.230.16.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.9.90	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
2.54.41.35	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
109.65.147.43	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
66.147.244.98	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
37.142.217.12	Israel	147.237.72.156	aman.idf.il	XSS - Basic 3	Block	1