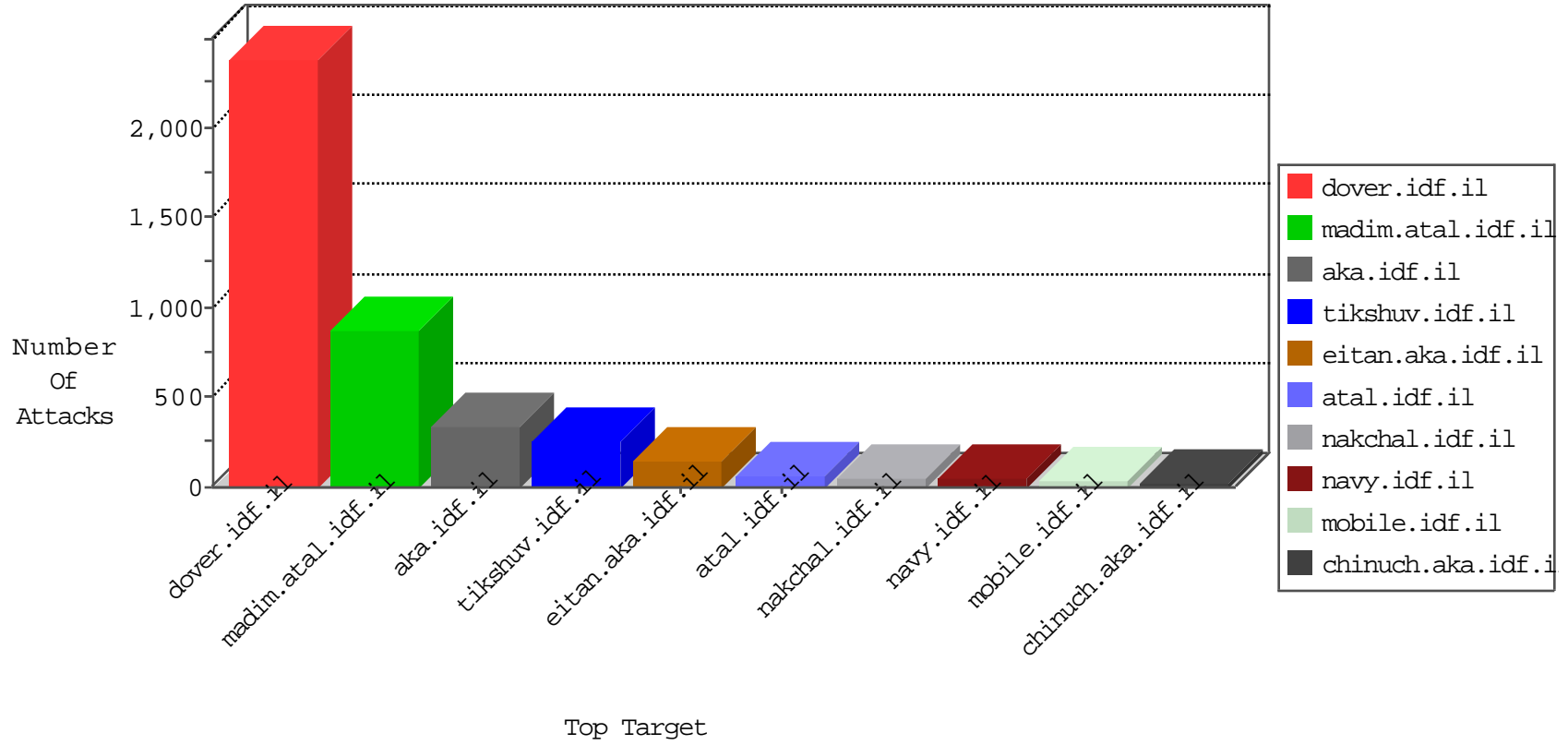


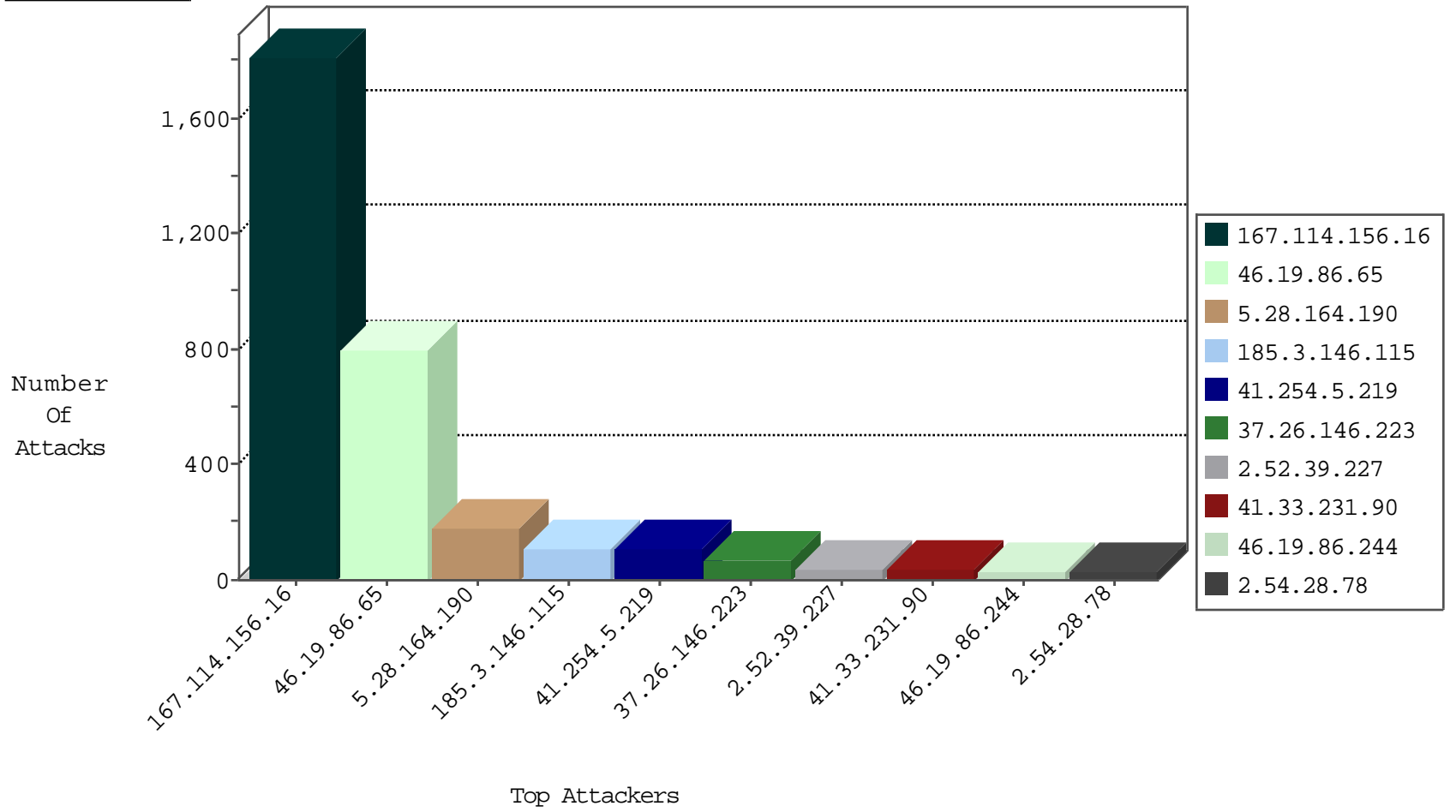
# IDF Under Attack Daily Report



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	3335
46.19.86.65	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	205
82.178.149.166	Oman	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	1
72.27.99.119	Jamaica	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
72.27.99.119	Jamaica	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
198.48.92.104	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
78.171.44.57	Turkey	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
148.251.178.31	Germany	147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	2
105.103.87.142	Algeria	147.237.77.216	dover.idf.i	3886: HTTP: Cross Site Scripting in POST Request	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
148.251.178.31	147.237.77.74	Germany	law.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.66.125	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
210.73.74.202	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
105.103.87.142	147.237.77.216	Algeria	dover.idf.il	SQL Injection - Select From	1
187.161.136.224	147.237.77.178	Mexico	e.matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
85.250.75.41	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.88	147.237.77.121		e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.88	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.88	147.237.8.46		e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
210.117.121.60	147.237.8.27	Korea, Republic of	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
151.217.178.55	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
210.73.74.202	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
210.73.74.202	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
117.25.155.164	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
210.73.74.202	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
117.25.155.164	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
105.103.87.142	147.237.77.216	Algeria	dover.idf.il	GPL WEB_SERVER /etc/passwd	1
176.13.13.50	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
151.217.178.88	147.237.77.74		law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.88	147.237.76.176		test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
210.117.121.60	147.237.8.27	Korea, Republic of	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
151.217.178.88	147.237.0.33		idf.il	ET SCAN Potential VNC Scan 5900-5920	1
210.73.74.202	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
151.217.146.30	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
210.73.74.202	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
125.44.214.222	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
210.73.74.202	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
117.25.155.164	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.3.146.115	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	105
41.254.5.219	Libyan Arab Janahiriya	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	76
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
41.254.5.219	Libyan Arab Janahiriya	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	31
2.52.39.227	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
185.120.126.10		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
118.69.78.196	Vietnam	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.52.39.227	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
176.13.22.61	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
84.94.56.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
66.249.64.119	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.65	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.244	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
79.180.188.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.182.223.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.13.50	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
176.13.13.50	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
185.120.125.5		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
185.32.179.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
5.22.134.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.22.61	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.156.163	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.149.188	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
31.168.16.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.203	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	6
109.67.220.69	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.86.85	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.102.233.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.183.123.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.140.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.253.145.235	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.123.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.26.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.160.226	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.102.254.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.29.176.147	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
146.185.234.48	Russian Federation	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.152.56	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.65	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.65	Block	438
5.28.164.190	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	181
46.19.86.65	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.86.65	Block	169
46.19.86.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	152
37.26.146.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
2.54.28.78	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
149.88.204.153	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
5.102.254.101	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
207.46.13.46	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
146.185.234.48	Russian Federation	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 146.185.234.48	Block	4
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	4
105.103.87.142	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.103.87.142	Block	4
109.253.209.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.6.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.24.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.106.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.88.213.192	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.88.213.192	Block	3
217.132.45.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.121.128.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
217.132.45.112	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302	Block	2
109.226.60.148	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mce_src=	Block	2
93.173.237.191	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.21.238	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
79.181.38.249	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.145.235	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.110.111.167	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.111.102.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.177.161.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.8.89	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
46.19.85.211	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
95.35.204.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.57.184	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
149.78.154.225	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.220.69	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
2.54.57.180	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.94.100.18	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
195.154.226.90	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
107.21.1.8	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.182.57.127	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
180.76.15.18	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.127.78.98	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
149.88.213.192	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/sachar	Block	1
46.19.85.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
66.147.242.172	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
5.29.176.147	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.228.62.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1