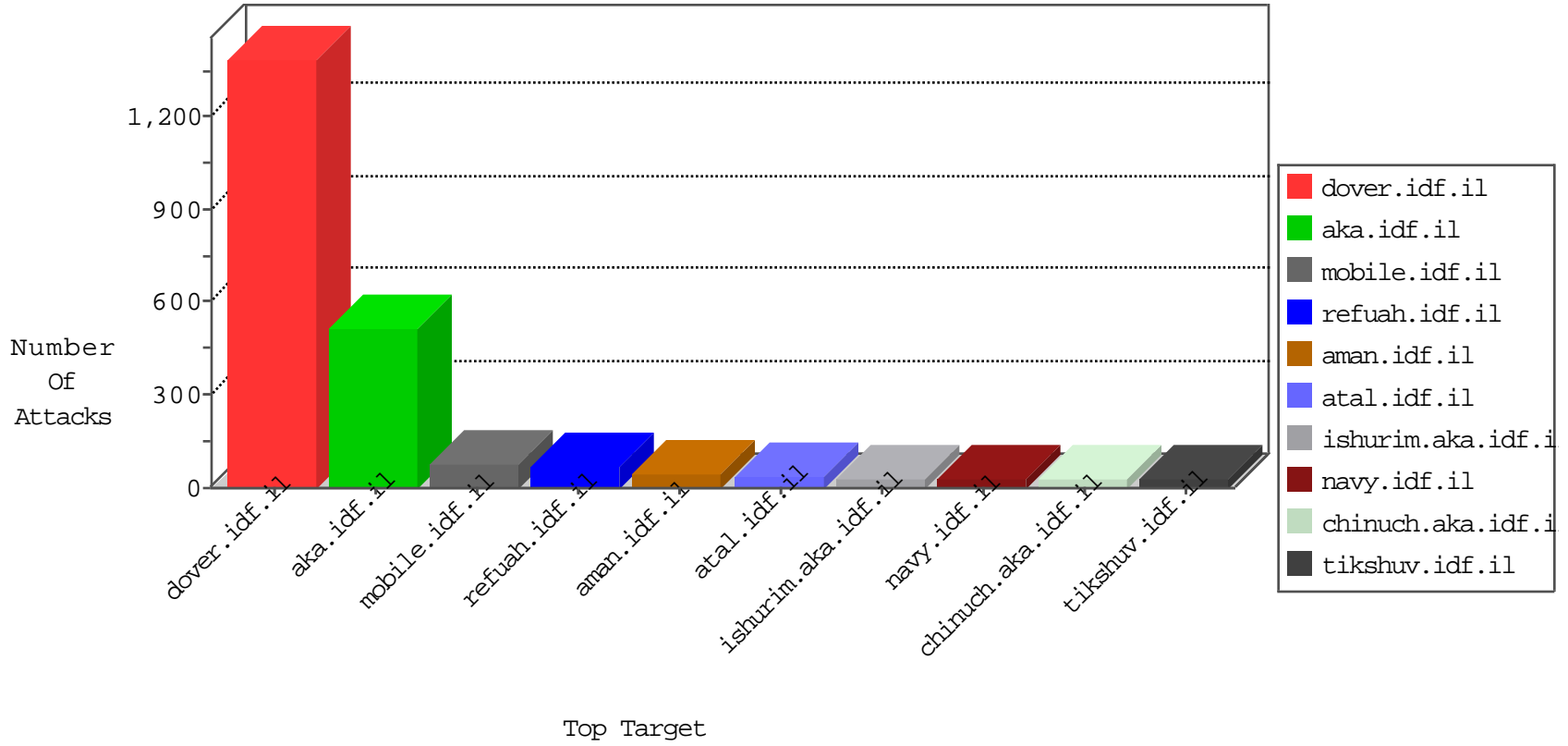


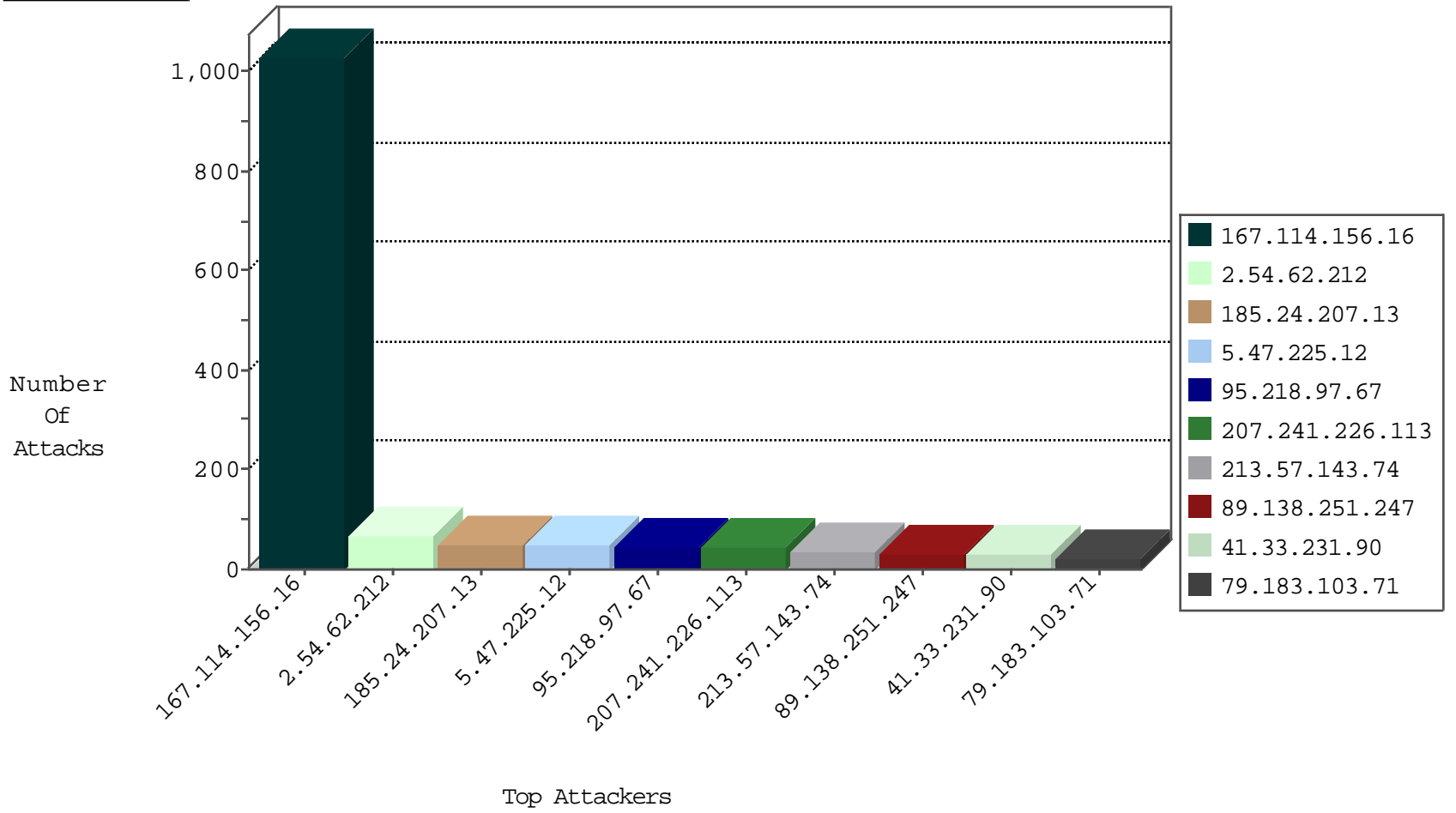
# IDF Under Attack Daily Report



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	3000
109.65.19.147	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
31.168.225.146	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
188.214.128.113	Romania	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	2
218.52.197.109	Korea, Republic of	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

12-30-2015-18:04:01 to 12-30-2015-19:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.216.115.6		147.237.77.216	dover.idf.	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
95.218.97.67	147.237.77.233	Romania	atal.idf.il	ET SCAN NMAP -sA (2)	4
95.218.97.67	147.237.77.216	Romania	dover.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
207.241.226.113	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	3
95.218.97.67	147.237.77.19	Romania	law-forum.idf.il	ET SCAN NMAP -sA (2)	2
95.218.97.67	147.237.77.234	Romania	halag.idf.il	ET SCAN NMAP -sA (2)	2
213.57.157.234	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.218.97.67	147.237.77.74	Romania	law.idf.il	ET SCAN NMAP -sA (2)	1
201.165.32.205	147.237.76.39	Mexico	mobile.meitav.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.172.186.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.106.94.126	147.237.76.30		himush.idf.il	ET SCAN Potential SSH Scan	1
87.68.55.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.6.189	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.3.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.11.201.3	147.237.72.217	Italy	e.idf.il	ET SCAN NMAP -f -sS	1
46.121.193.15	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.99.215	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.254.65.9	147.237.72.166	Romania	aka.idf.il	portscan: TCP Distributed Portscan	1
213.151.39.137	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.218.97.67	147.237.77.205	Romania	prisha.idf.il	ET SCAN NMAP -sA (2)	1
89.138.205.219	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.106.94.126	147.237.8.14		e.orchot.idf.il	ET SCAN Potential SSH Scan	1
85.64.79.241	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.11.201.3	147.237.72.217	Italy	e.idf.il	ET SCAN NMAP -sS window 2048	1
79.177.114.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.160.149.162	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
40.115.57.147	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
5.28.129.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.218.97.67	147.237.77.227	Romania	e.hamaz.idf.il	ET SCAN NMAP -sA (2)	1
95.218.97.67	147.237.77.212	Romania	e.dover.idf.il	ET SCAN NMAP -sA (2)	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.62.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	42
89.138.251.247	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
207.241.226.113	United States	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	29
5.47.225.12	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
185.24.207.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
37.26.146.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
185.24.207.13	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
79.183.103.71	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
46.19.85.187	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
46.19.85.5	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
46.19.85.184	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
213.57.143.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
198.204.249.34	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.181.4.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
213.57.143.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
213.57.143.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
46.19.85.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.47.225.12	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	10
93.172.186.22	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
185.24.207.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.178.119.7	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.78.25.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.39.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.127.245.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
157.55.2.153	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.47.225.12	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.54.62.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.47.225.12	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.62.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
37.46.39.229	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.36	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.62.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
5.22.131.91	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.129.222	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.210.188.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.214.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.136.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.129.222	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.4.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.129.222	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
207.241.226.113	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
94.230.86.177	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.93.117	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
2.52.15.115	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	11
40.77.167.77	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
85.65.60.211	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	5
66.249.66.52	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
85.65.77.55	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	4
84.94.39.176	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
2.54.39.144	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
77.125.153.233	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.67.114.42	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	3
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
66.249.66.55	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.253.213.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.61	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.180.48.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.56.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
217.132.3.13	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPersonalId in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	2
109.253.202.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.127.126.6	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
109.65.140.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.139.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.127.182.224	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/registrationwizard/register.aspx parameter	None	2
37.26.149.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.69.222.188	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
95.86.121.165	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
109.253.207.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.26.146.250	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
212.150.214.90	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.aspx/getauthuser	Block	2
176.13.23.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.68.49.14	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
197.35.104.12	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
46.116.201.75	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
79.179.220.58	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.3.144.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.201.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
37.26.147.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.138.251.247	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.13.8.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.227	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.64.21.111	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$tfasimSignAll in www.aka.idf.il/main/sachar/payslips.aspx	None	1
213.57.178.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.120.69.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.196.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.123.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
187.161.116.239	Mexico	147.237.77.233	atal.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
178.154.189.37	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1