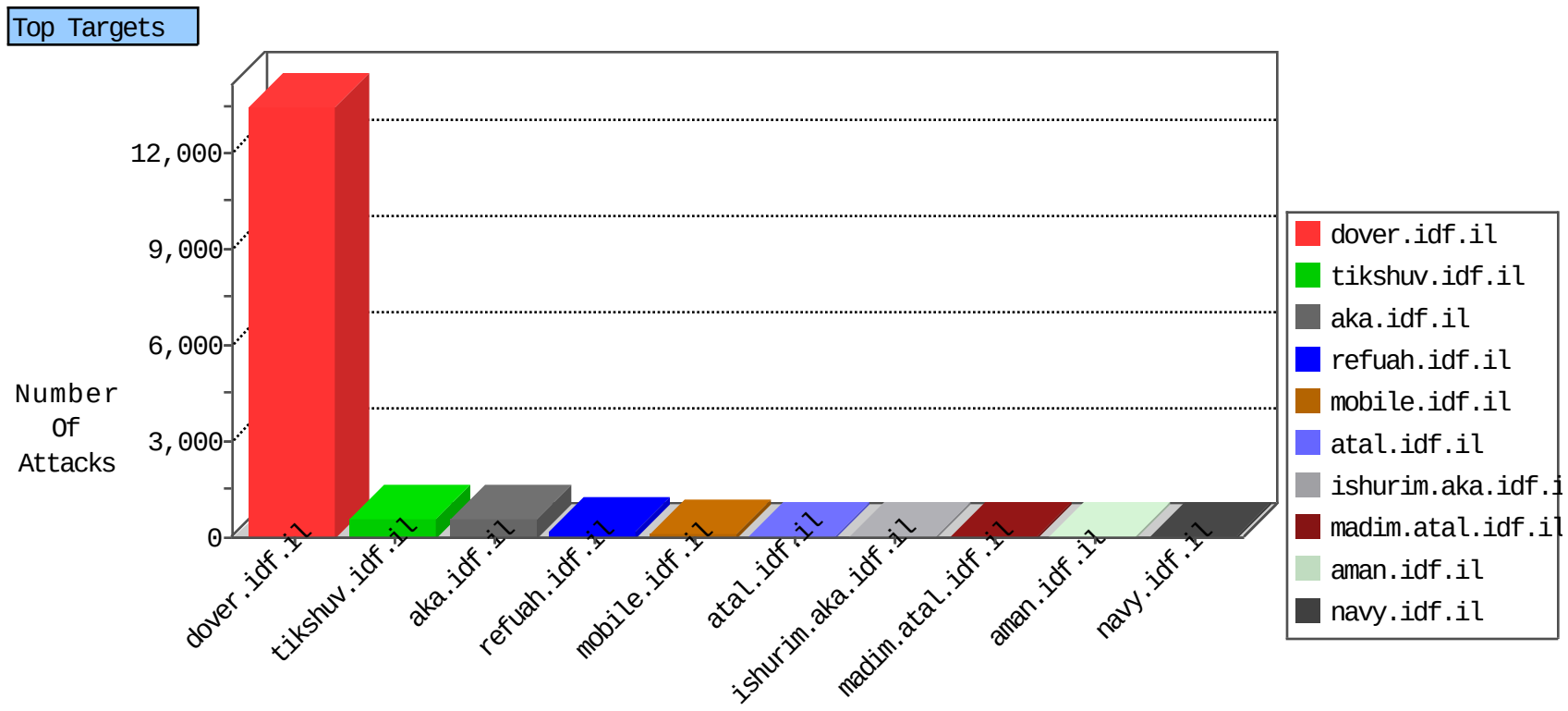
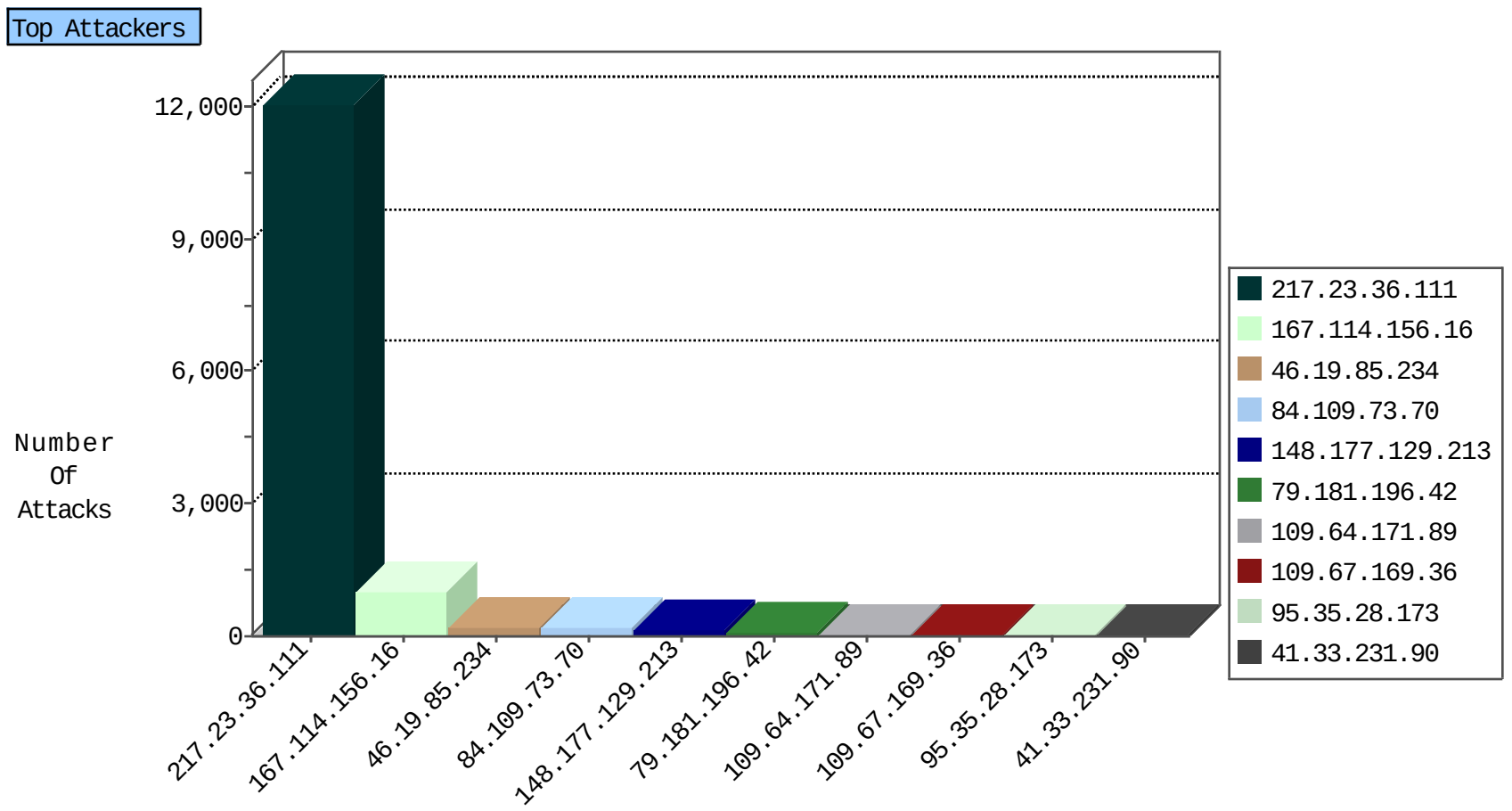
12-30-2015-15:04:04 to 12-30-2015-16:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-30-2015-15:04:04 to 12-30-2015-16:04:04

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	3017
62.219.224.61	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
212.179.210.163	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.182.20.205	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
148.177.129.213	Europe	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	3
148.177.129.213	Europe	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	2
195.6.5.35	France	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
94.102.56.238	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
94.102.56.238	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
101.226.142.209	China	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

12-30-2015-15:04:04 to 12-30-2015-16:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-30-2015-15:04:04 to 12-30-2015-16:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	2
91.201.236.114	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.197.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.39.169	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.163.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.76.202	Cote D'Ivoire	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
46.19.86.114	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.76.202	Cote D'Ivoire	e.halag.idf.il	ET SCAN NMAP -f -sS	1
2.54.128.146	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.3.87	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.14.42	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.238.160.101	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 3072	1
85.250.234.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.23.36.111	147.237.77.216	Jordan	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.243.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.76.202	Cote D'Ivoire	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
46.19.85.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
168.62.238.153	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.55	147.237.0.19		madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
109.66.108.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

12-30-2015-15:04:04 to 12-30-2015-16:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
217.23.36.111	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1209
148.177.129.213	Europe	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	125
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
213.57.135.41	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
77.127.204.121	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.86.199	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	19
37.26.148.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
176.12.141.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
96.44.187.158	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
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	14
84.109.98.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.147.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
95.35.28.173	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
46.19.85.0	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
84.108.52.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	11
84.108.52.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
213.57.143.49	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
80.246.139.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
79.179.62.113	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
80.249.65.135	Algeria	147.237.77.216	dover.idf.il	drop		drop	10
95.35.28.173	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
46.19.86.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.177.35.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.234	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
213.57.143.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
217.23.36.111	Jordan	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	8
188.209.52.109	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.130.9	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
95.35.28.173	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
109.186.185.87	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
169.254.131.94		147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
84.228.220.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.212	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
213.8.204.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.234	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.46.39.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.147.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.133.127	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.234	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.22.129.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.12.136.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.130.117	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.23.36.111	Jordan	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	3626
217.23.36.111	Jordan	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 217.23.36.111	Block	3625
217.23.36.111	Jordan	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	3614
46.19.85.234	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	190
84.109.73.70	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	186
79.181.196.42	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	101
109.67.169.36	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 109.67.169.36	Block	41
176.13.19.39	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	4
176.12.141.95	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
40.77.167.77	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
2.54.128.146	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	4
109.253.140.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
192.114.105.254	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 192.114.105.254	Block	4
2.54.128.146	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	4
109.64.171.89	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 109.64.171.89	Block	3
109.64.171.89	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 109.64.171.89	Block	3
46.19.86.99	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	3
109.64.171.89	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 109.64.171.89	Block	3
109.253.146.185	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.64.171.89	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 109.64.171.89	Block	3
109.64.171.89	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 109.64.171.89	Block	3
176.13.1.80	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	3
109.64.171.89	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 109.64.171.89	Block	3
109.64.171.89	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 109.64.171.89	Block	3
192.114.105.254	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
185.32.179.195	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.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.26.149.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.109	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.76.96.51	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.54.151.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.10.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.56.118	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
37.26.147.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
81.218.131.215	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many of the Same Response Code (404) in Session from 81.218.131.215	Block	2
46.19.86.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
95.35.156.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.8.204.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.28.155.188	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	2
109.64.171.89	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.52.168.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.183.50.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.136.145	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.52	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.86.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.64.171.89	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 109.64.171.89	Block	2
46.19.85.113	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
176.13.18.18	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	2