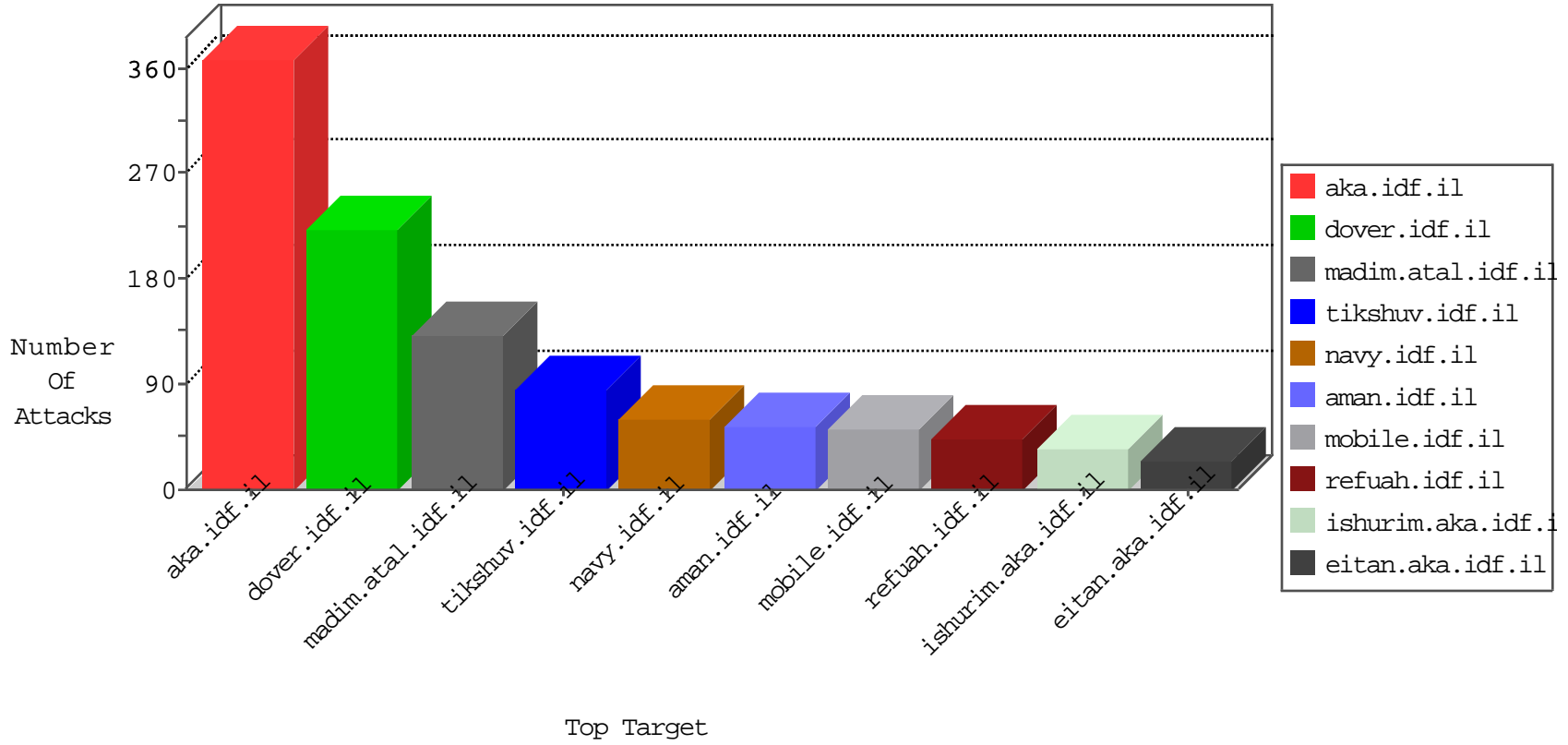


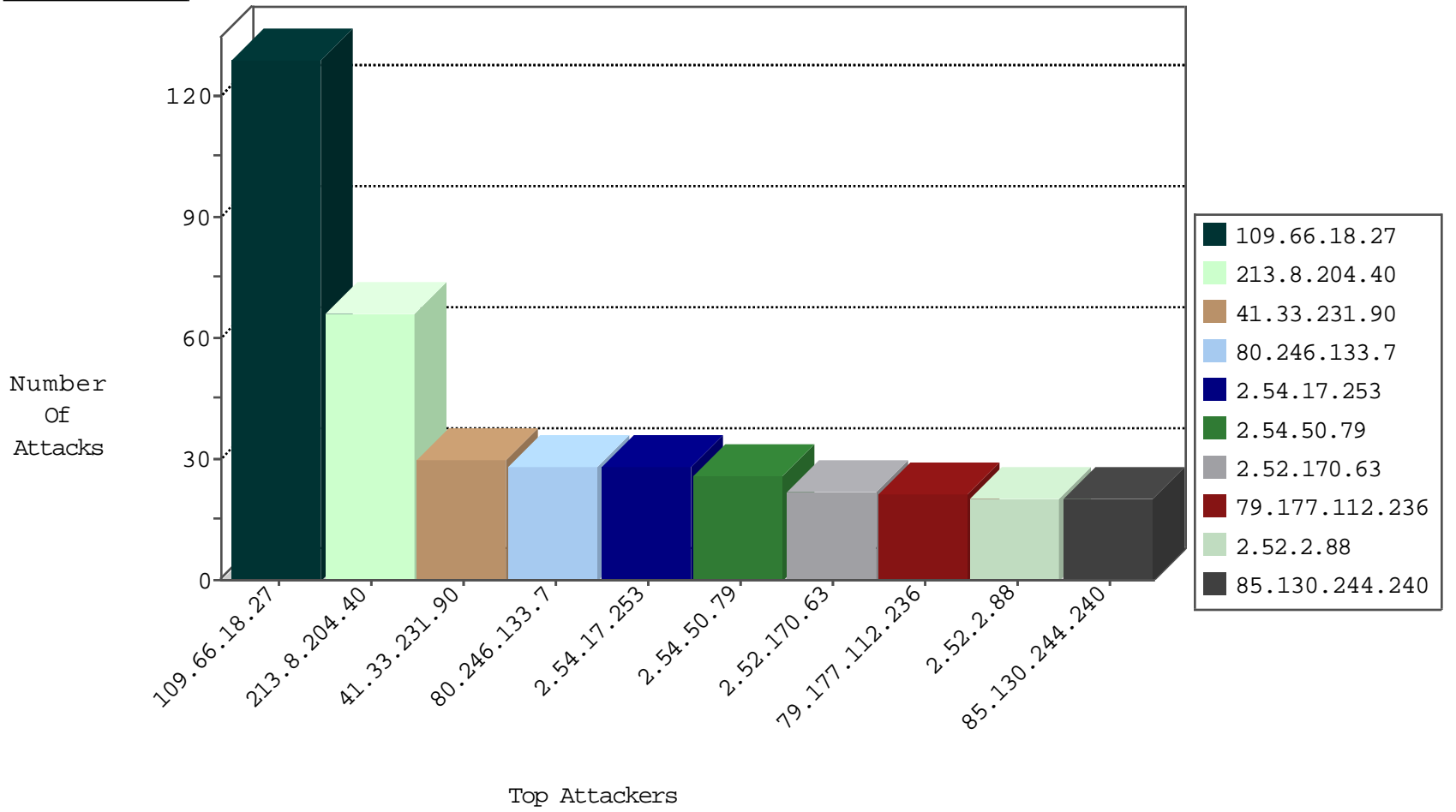
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.17.253	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	11
31.131.4.153	Moldova, Republic of	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
207.46.13.127	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
115.239.228.10	China	147.237.76.39	mobile.meitav.idf.il	JLM_Purple_Con_Limit_Http	drop	3
218.6.50.50	China	147.237.76.200	eitan.aka.idf.il	Invalid TCP Flags	drop	2
115.239.228.10	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	2
37.26.146.162	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2
180.97.106.37	China	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.37	China	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
107.150.33.58	United States	147.237.77.216	dover.idf.il	block-sp-traffic	drop	1
123.235.28.156	China	147.237.77.205	prisha.idf.il	Invalid TCP Flags	drop	1
185.130.5.179		147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
107.150.33.59	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traffic	forward	1
173.208.206.202	United States	147.237.72.156	aman.idf.il	block-sp-traffic	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.219.9	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.120.173.130	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	7
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
87.71.23.36	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
37.26.147.150	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
149.78.200.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
69.30.213.18	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
149.88.3.143	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
31.131.4.153	Moldova, Republic of	147.237.76.86	navy.idf.il	0543: HTTP: php.cgi Access	Block	1
92.198.27.76	Germany	147.237.72.166	aka.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
31.131.4.153	Moldova, Republic of	147.237.77.216	dover.idf.il	0543: HTTP: php.cgi Access	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	2
2.54.7.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.112.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.186.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.92.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.50.93.19	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.51.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.216	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
37.26.148.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.185.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.23.87	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.81.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.137.8	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.146.64	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.141.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.127.87.85	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.176.168.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.142.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.88.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.139.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.60.41.104	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.6.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.203	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.144	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
37.26.146.241	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.95.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
80.246.133.7	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
79.177.112.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
82.145.209.158	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
2.52.2.88	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
85.130.244.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
176.13.5.214	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.170.63	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
185.86.162.20		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.147.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
62.0.207.1	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	7
85.64.115.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.158.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.17.230	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.172	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.134.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.82	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.148.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.57	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.82	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
46.19.85.146	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.50.79	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.50.79	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
140.147.249.7	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.54.50.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.50.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.50.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
157.55.2.167	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
188.161.13.84	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.246.136.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
2.54.17.253	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.151.35.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.177.246.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.23.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.253.213.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.170.63	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
109.186.133.253	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
84.228.254.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.182.139.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.148.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.234.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.114.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.18.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	128
213.8.204.40	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 213.8.204.40	Block	64
87.68.148.113	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	9
85.64.115.178	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Email in mobile.idf.il/sachar/createaccount	Block	5
93.173.117.103	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	3
82.166.22.37	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 82.166.22.37	Block	3
213.57.240.91	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
213.57.240.91	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	2
212.76.104.60	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22015-he/dover.aspx&sa=u&ved=0ahukewjx-dtjhozlahu cdiwkhdgkcjoqfggbmay&usg=afqjcnfyuwzavvad7pf31tnvl_1-ne2elq	Block	2
31.131.4.153	Moldova, Republic of	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 31.131.4.153	Block	2
84.110.32.90	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
213.57.240.91	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
157.55.39.132	United States	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
109.253.138.225	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
93.173.117.103	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 93.173.117.103	Block	2
207.46.13.36	United States	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
213.57.240.91	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	2
31.131.4.153	Moldova, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.131.4.153	Block	2
213.57.240.91	Israel	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	2
5.22.134.229	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
46.117.171.204	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
157.55.39.222	United States	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
2.52.169.223	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
81.218.135.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
157.55.39.110	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1360-he/atal.aspx	Block	1
46.19.86.199	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
93.172.225.50	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.84.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
87.68.156.31	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
213.8.204.37	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.181.148.53	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
109.253.131.24	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
37.26.146.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
84.228.254.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
199.30.24.245	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.177.215.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
109.66.34.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.117.171.204	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
2.54.155.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
84.94.61.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
176.13.1.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
80.179.5.19	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
149.78.77.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.86.19	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
89.138.22.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
213.57.141.107	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 213.57.141.107 (Unknown SSL Session)	None	1
79.179.229.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
109.66.134.19	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1