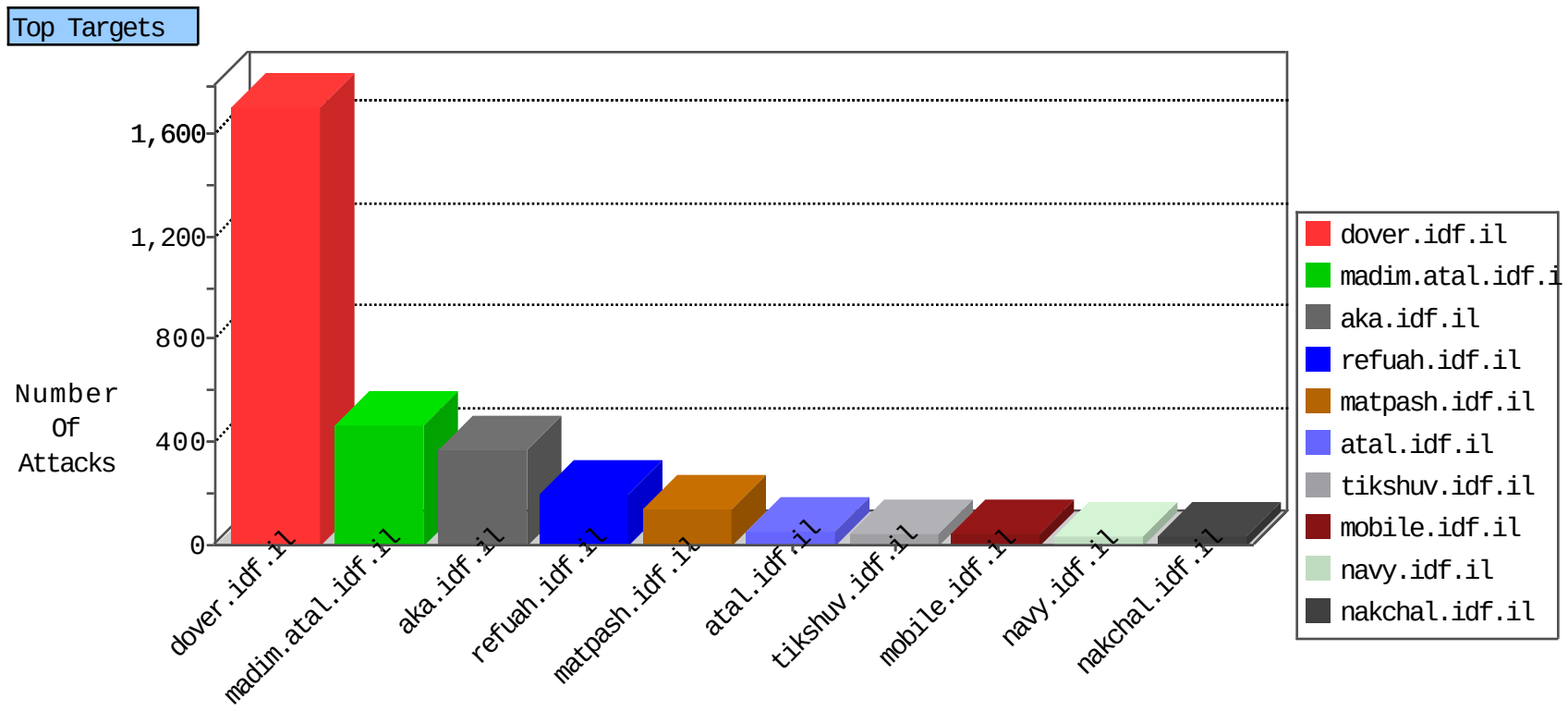
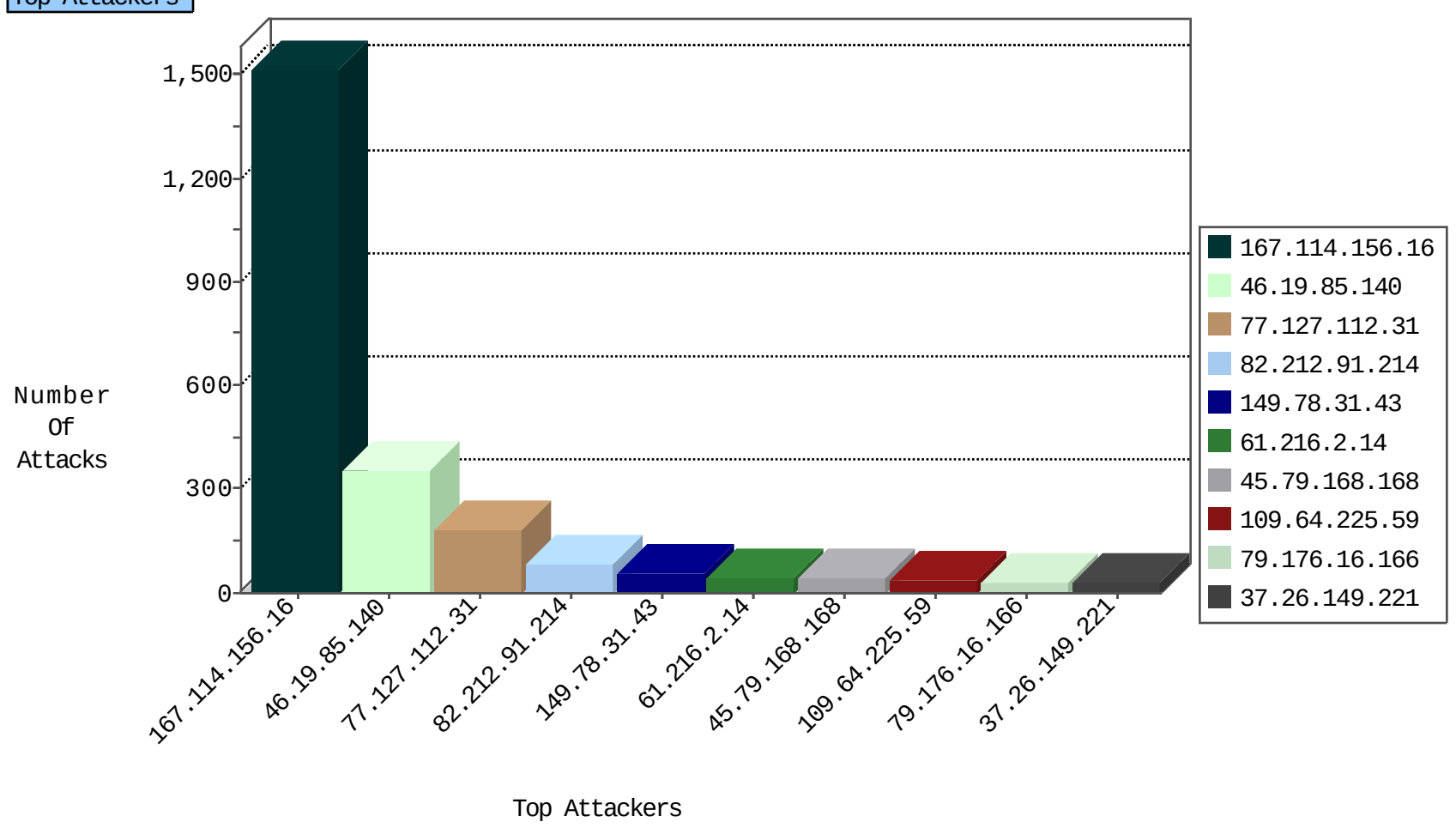
01-10-2016-14:04:05 to 01-10-2016-15:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-10-2016-14:04:05 to 01-10-2016-15:04:05

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	3150
66.249.73.214	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	293
79.180.111.59	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.10	China	147.237.0.33	idf.il	Frk_Under_Attack_Con_Http	drop	2
115.230.124.164	China	147.237.76.200	eitan.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
208.67.1.66	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
202.112.51.96	China	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1
202.112.51.96	China	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
202.112.51.96	China	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
208.67.1.66	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
202.112.51.96	China	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	drop	1
202.112.51.96	China	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
202.112.51.96	China	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
202.112.51.96	China	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
202.112.51.96	China	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	drop	1
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
202.112.51.96	China	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
202.112.51.96	China	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
115.239.228.10	China	147.237.0.33	idf.il	Frk_Purple_Con_Limit_Http	drop	1
202.112.51.96	China	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
202.112.51.96	China	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	drop	1

01-10-2016-14:04:05 to 01-10-2016-15:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.75	United States	147.237.8.14	e.orchot.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-10-2016-14:04:05 to 01-10-2016-15:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
93.174.93.203	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.222.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.204.188.142	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
37.26.147.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.76.30	Sweden	himush.idf.il	ET SCAN NMAP -sS window 1024	1
158.255.6.220	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.142.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.0.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.216.2.14	147.237.0.17	Taiwan	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.62.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.77.79.38	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
158.255.6.220	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
149.88.238.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-10-2016-14:04:05 to 01-10-2016-15:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.127.112.31	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	180
82.212.91.214	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	83
45.79.168.168		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	42
79.176.16.166	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
109.64.225.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
37.26.149.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
84.108.184.54	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
79.182.10.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.192.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.64.225.59	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	10
66.249.78.37	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.161	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
217.132.138.98	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	9
61.216.2.14	Taiwan	147.237.0.17	m.my-kosher-kravi.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	9
192.118.27.253	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.67.157.34	Israel	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
5.102.253.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
84.229.244.6	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.68.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.33.101	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
89.138.46.160	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.182.10.130	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
84.229.244.6	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	5
46.19.85.32	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.118.27.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
65.55.210.77	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.149.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.146	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.118.27.253	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.52.182.140	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
149.78.127.1	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
80.179.114.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
62.219.167.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.179.176.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
176.13.21.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.179.9.245	Israel	147.237.76.31	nakchal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.177.59.65	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.64.135.155	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
79.182.51.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.2.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.209.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.140	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.140	Block	195
46.19.85.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	162
149.78.31.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
80.246.136.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
109.67.157.34	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	9
212.179.9.245	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 212.179.9.245	Block	7
37.26.149.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.36.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.50.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
212.179.9.245	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	6
188.143.232.22	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.22	Block	5
77.127.238.206	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
109.253.157.166	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
109.253.144.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
91.207.90.10	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.207.90.10	Block	3
37.26.149.221	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.182.8.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	3
195.154.227.118	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	2
217.132.147.106	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
149.88.145.165	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
46.19.86.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.94.159.219	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	2
5.29.148.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.204	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
213.57.189.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.218.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	2
46.19.85.40	Israel	147.237.0.34	tikshuv.idf.il	Multiple Abnormally Long Request from 46.19.85.40	Block	1
80.246.136.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
79.178.2.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
61.216.2.14	Taiwan	147.237.77.226	www.chamatz.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
91.199.69.254	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
217.132.138.98	Israel	147.237.76.86	navy.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 217.132.138.98	Block	1
84.108.39.48	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
212.235.103.211	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 212.235.103.211	Block	1
2.54.184.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
71.28.188.58	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Value	Block	1
149.88.127.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
132.70.66.10	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
81.218.116.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.76.105.88	Israel	147.237.72.166	aka.idf.il	Unknown Parameter sa in www.aka.idf.il/main/haredim/general.aspx	None	1