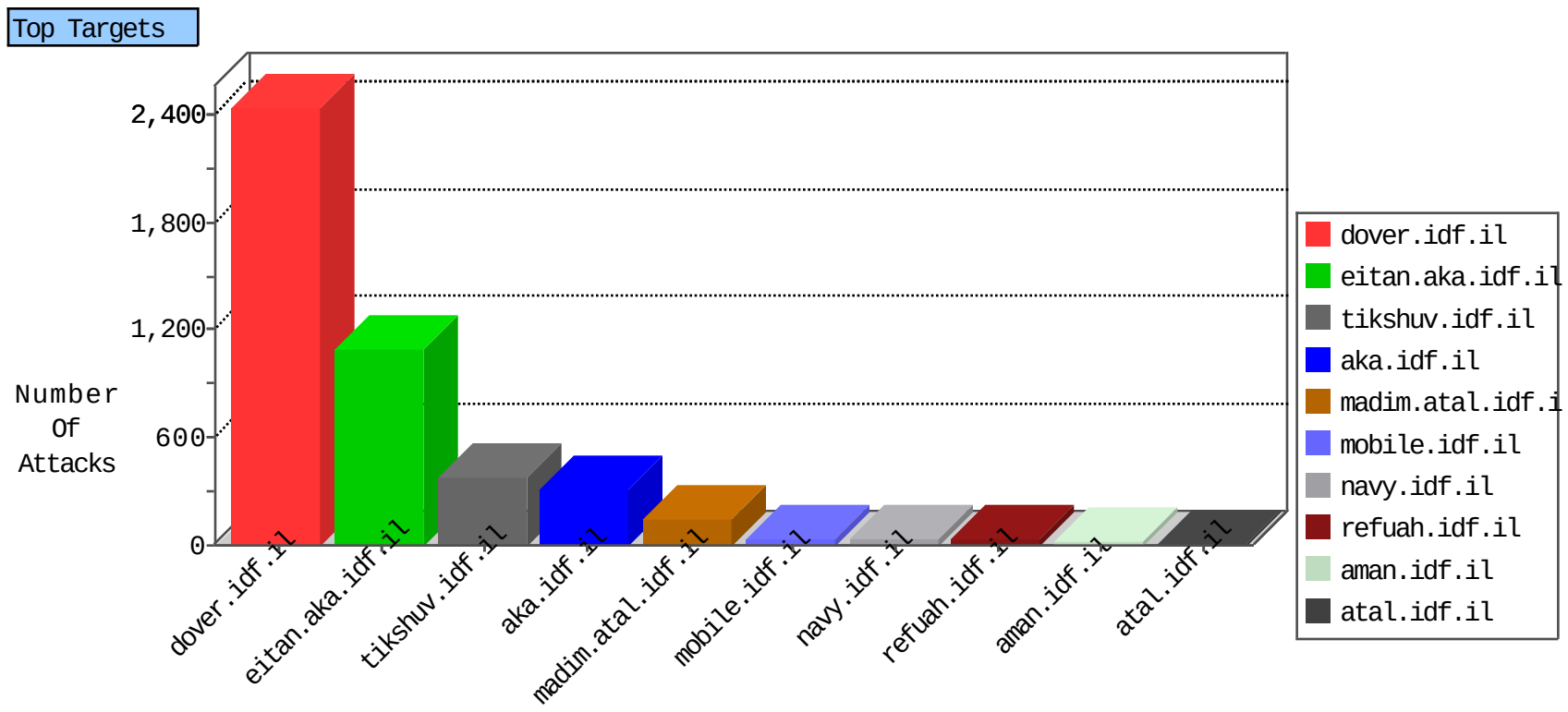
12-22-2015-14:04:06 to 12-22-2015-15:04:06

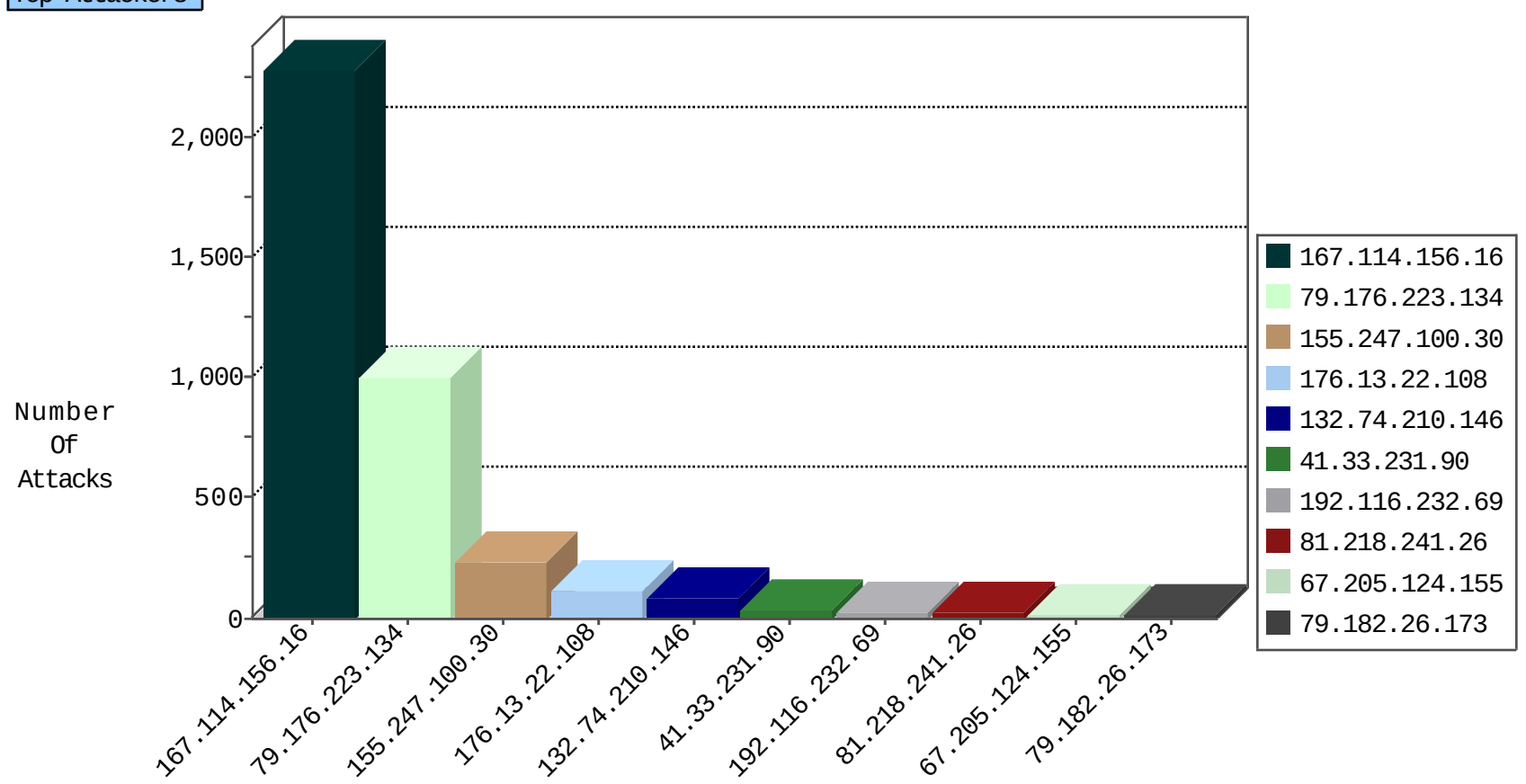
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

12-22-2015-14:04:06 to 12-22-2015-15:04:06

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	3148
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102

12-22-2015-14:04:06 to 12-22-2015-15:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.250.27.93	Russian Federation	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

12-22-2015-14:04:06 to 12-22-2015-15:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.216.19.183	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
85.64.85.101	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.28.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.106.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.69.30.108	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
182.75.6.126	147.237.76.176	India	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
154.5.154.26	147.237.72.166	Canada	aka.idf.il	portscan: TCP Distributed Portscan	1
125.211.216.68	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
92.222.242.108	147.237.0.19	France	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.51.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.46.189	147.237.72.166	Israel	aka.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
176.0.62.174	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.113.190	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
92.222.242.108	147.237.72.156	France	aman.idf.il	ET SCAN NMAP -sS window 1024	1

12-22-2015-14:04:06 to 12-22-2015-15:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.176.223.134	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	864
155.247.100.30	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	234
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
79.182.26.173	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
95.245.235.193	Italy	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
67.205.124.155	Canada	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	14
132.74.210.146	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
218.205.17.172	China	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
218.205.17.207	China	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.177.206.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
209.88.175.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
185.3.146.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.223	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.114.91.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.25.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.22.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.126.115		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.191.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.72.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.242.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.146.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.173	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.242.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.120.126.12		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.194.199.151	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
31.154.174.220	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
209.88.175.166	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
85.65.2.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
82.80.218.76	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.186.184.18	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.22.108	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.203.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.108	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.228.42.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.218.76	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.64.18.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.193	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.53.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.206.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.64.114	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
79.176.223.134	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	134
176.13.22.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
132.74.210.146	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 132.74.210.146	Block	46
176.13.22.108	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.22.108	Block	35
192.116.232.69	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	21
132.74.210.146	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
37.26.148.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
218.205.17.204	China	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	6
172.246.226.45	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	5
52.4.53.92	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	5
109.253.213.238	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	5
46.19.86.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
218.205.17.158	China	147.237.0.34	tikshuv.idf.il	Distributed Parameter Type Violation on www.tikshuv.idf.il/modules/forums/forum.aspx parameter FolderId	Block	4
91.200.219.248	Russian Federation	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	3
194.90.156.133	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 194.90.156.133	Block	3
190.198.251.245	Venezuela	147.237.0.34	tikshuv.idf.il	Distributed Parameter Type Violation on www.tikshuv.idf.il/modules/forums/forum.aspx parameter FolderId	Block	3
200.121.137.229	Peru	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	3
67.205.124.155	Canada	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	3
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	3
212.199.57.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.172.21.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
162.216.19.183	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 162.216.19.183	Block	3
52.4.53.92	United States	147.237.0.34	tikshuv.idf.il	Distributed Parameter Type Violation on www.tikshuv.idf.il/modules/forums/forum.aspx parameter FolderId	Block	3
79.177.206.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
195.145.216.49	Germany	147.237.0.34	tikshuv.idf.il	Distributed Parameter Type Violation on www.tikshuv.idf.il/modules/forums/forum.aspx parameter FolderId	Block	3
172.246.226.124	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	3
162.216.19.183	United States	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	3
132.74.210.146	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	3
91.200.219.248	Russian Federation	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/901-8581-he/tikshuv.aspx#.vnmqevl96uk	Block	3
195.145.216.49	Germany	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	3
162.216.19.183	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/404testpage4525d2fdc	Block	3
176.13.0.161	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
66.249.65.80	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
79.134.207.190	Russian Federation	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	2
172.246.226.148	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/901-8581-he/tikshuv.aspx#.vnmqevl96uk	Block	2
221.178.182.132	China	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	2
186.90.119.236	Venezuela	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	2
84.228.42.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
155.247.100.30	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	2
46.19.85.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.169.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.81.45.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
77.20.138.34	Germany	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	2
91.199.69.254	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 91.199.69.254	Block	2
117.169.66.249	China	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	2
41.169.8.2	South Africa	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	2
79.134.207.190	Russian Federation	147.237.0.34	tikshuv.idf.il	Distributed Illegal HTTP Version	Block	2
194.90.15.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
144.76.51.118	Germany	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	2
79.134.207.190	Russian Federation	147.237.0.34	tikshuv.idf.il	Distributed Malformed URL	Block	2