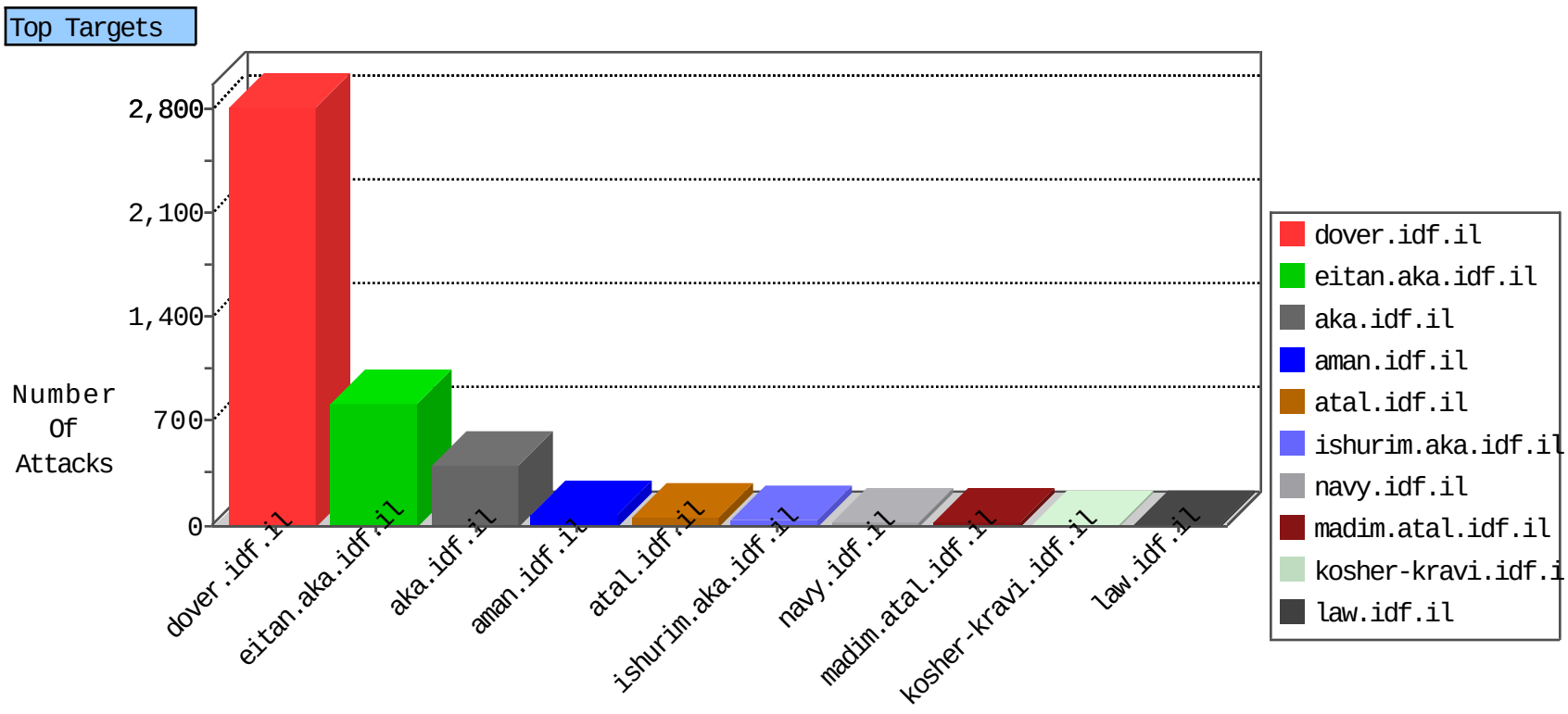
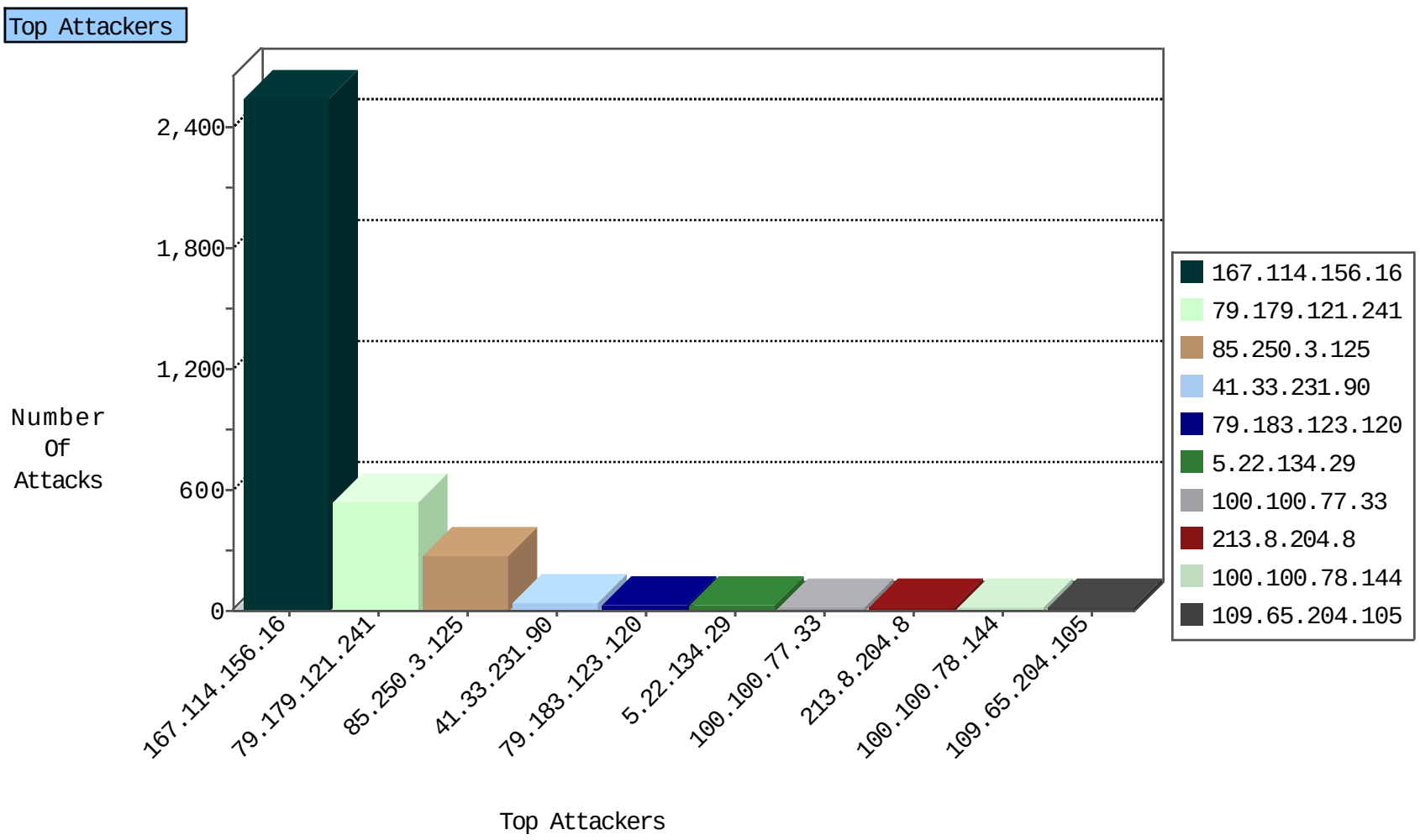
12-01-2015-21:04:05 to 12-01-2015-22:04:05

IDF Under Attack
Daily Report





12-01-2015-21:04:05 to 12-01-2015-22:04:05

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	3379
66.249.66.81	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	149
79.183.4.68	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
112.198.79.54	Philippines	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

12-01-2015-21:04:05 to 12-01-2015-22:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
59.58.107.199	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
195.154.188.158	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.188.186	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.216.86	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

12-01-2015-21:04:05 to 12-01-2015-22:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.154.216.86	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	4
195.154.216.86	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS) .asp Filename Extension Parsing File Upload Security Bypas Attempt (asp)	4
195.154.216.86	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
37.142.167.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.154.188.158	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	1
106.3.45.131	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
223.4.210.53	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.154.188.158	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	1
1.175.101.192	147.237.0.35	Taiwan	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.195	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
212.150.62.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.154.216.86	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP phptest.php access	1
94.102.48.195	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
183.82.47.172	147.237.8.50	India	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
79.181.99.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.252.84	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
79.177.35.148	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.119.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
69.79.227.85	147.237.72.166	Puerto Rico	aka.idf.il	portscan: TCP Distributed Portscan	1
195.154.188.224	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	1
106.3.45.131	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.154.188.186	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP phptest.php access	1
106.3.45.131	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.130.145.216	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.188.158	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP phptest.php access	1
106.3.45.131	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
223.4.210.53	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.154.188.158	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	1
37.142.64.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
223.4.210.53	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.154.188.158	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS) .asp Filename Extension Parsing File Upload Security Bypas Attempt (asp)	1
208.80.155.223	147.237.77.74	United States	law.idf.il	Tehila - Perl LWP with fake user agent	1
94.102.48.195	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
185.3.146.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.164.246	147.237.72.156	Israel	aman.idf.il	portscan: TCP Distributed Portscan	1
183.82.47.172	147.237.8.50	India	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.216.86	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	1
79.180.203.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
159.147.148.28	147.237.76.201	Spain	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
77.126.12.14	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.154.188.224	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	1
109.65.105.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.61	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
195.154.188.224	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS) .asp Filename Extension Parsing File Upload Security Bypas Attempt (asp)	1
106.3.45.131	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
62.219.115.17	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.154.188.186	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	1

12-01-2015-21:04:05 to 12-01-2015-22:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.179.121.241	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	480
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	22
213.8.204.8	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
100.100.108.24		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
46.19.86.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
79.183.123.120	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	15
79.183.123.120	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
5.22.134.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
79.178.170.192	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.11.98		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
5.22.134.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
84.229.161.2	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
100.100.78.144		147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	10
79.177.164.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.57.143.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
37.142.68.16	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.21	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
31.168.125.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.78.144		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.142.110.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
100.100.95.54		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
37.142.110.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.122.142	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.177.173.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.59	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.250.3.125	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.148.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.111.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.145.218.139	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
93.173.184.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.28.160.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.26.147.236	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.142.68.16	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.65.113.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.12.144.142	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.57.193.130	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.254.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
100.100.78.144		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.250.3.125	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	260
79.179.121.241	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
109.65.204.105	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.65.204.105	Block	17
176.12.149.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
132.72.138.1	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 132.72.138.1	Block	8
46.121.198.248	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
79.182.131.89	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.182.131.89	Block	5
176.12.137.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.88.140.78	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	3
37.26.149.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.106.63	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
87.69.87.39	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation __EVENTVALIDATION in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	3
74.71.0.154	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
87.69.87.39	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
95.86.124.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.124.44	Block	2
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.65.11.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
95.86.82.228	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/undefined/	Block	2
5.28.130.217	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	2
85.64.243.192	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
85.244.122.252	Portugal	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
46.117.245.123	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
149.88.140.78	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/sip_storage/files/7	Block	1
79.182.131.89	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
37.26.148.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.214.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.178.77	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
95.86.103.76	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH)	None	1
77.125.81.115	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
176.13.3.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/1133-20752-he/idfgdover.aspx	Block	1
157.55.39.17	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16602-en/dover	Block	1
46.19.85.215	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
84.94.161.14	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 84.94.161.14	None	1
212.150.174.186	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/saiarotflash.aspx	Block	1
79.179.96.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.19.32	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.102.206.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized Method GET for www.aka.idf.il/iturim/asp/searchresults.asp	Block	1
2.52.53.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.107.8.79	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
85.244.122.252	Portugal	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
46.121.110.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.54.178.77	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
77.126.236.228	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 77.126.236.228 (Unknown SSL Session)	None	1
176.13.3.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.32	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/telerik.web.ui.webresource.axd	Block	1