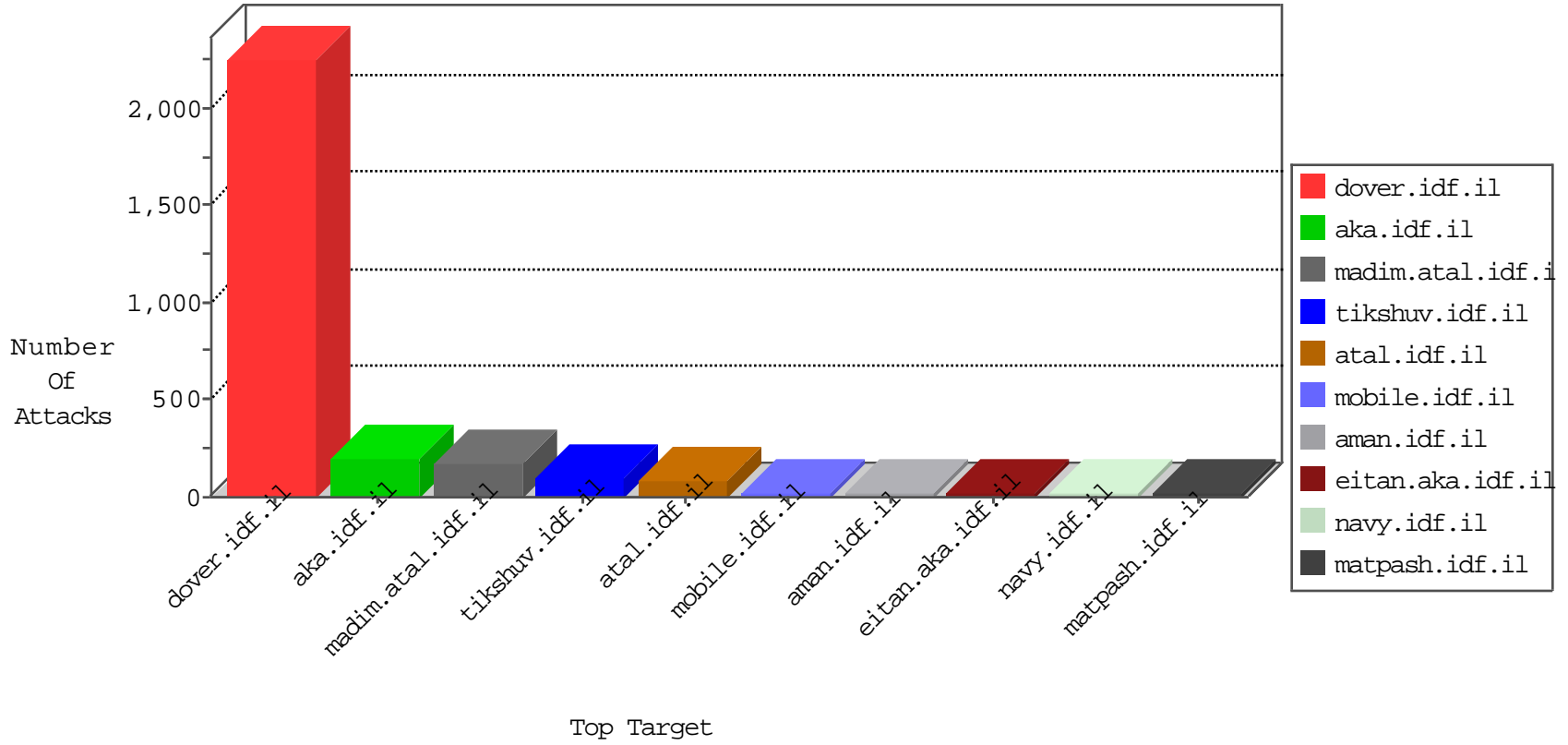


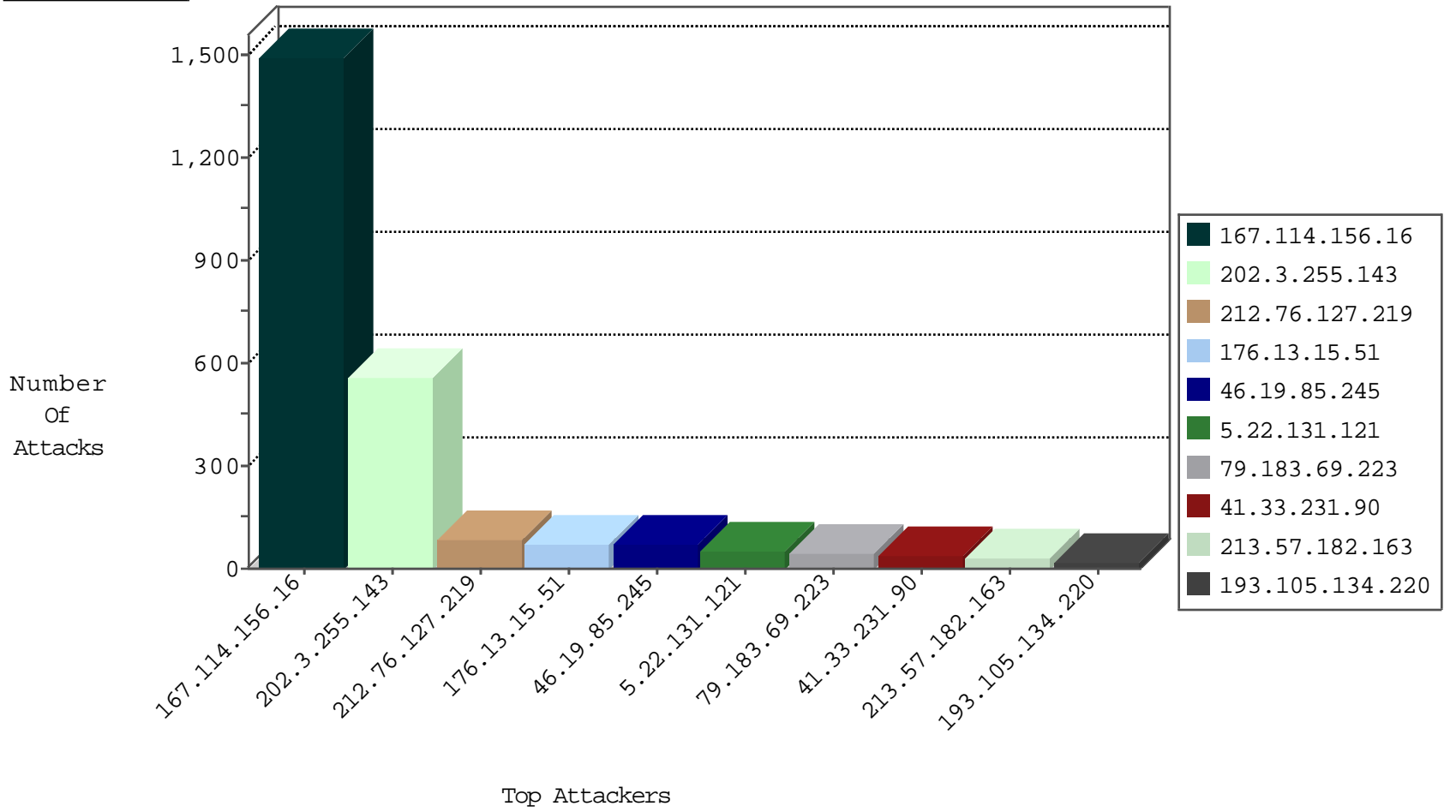
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3173
2.52.14.136	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
212.179.54.237	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
79.183.168.79	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
188.120.133.211	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
66.102.9.118	United States	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
185.130.5.224		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

01-17-2016-22:04:09 to 01-17-2016-23:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.75	United States	147.237.76.202	e.halag.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	520
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
213.8.204.20	147.237.76.30	Israel	himush.idf.il	ET SCAN NMAP -sA (2)	2
66.240.192.138	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
200.188.148.124	147.237.0.15	Mexico	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
168.62.238.153	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
95.86.72.221	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
71.6.165.200	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.240.236.119	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
66.240.236.119	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.240.192.138	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
200.188.148.124	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
199.119.248.71	147.237.0.33	Puerto Rico	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
168.62.238.153	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
160.176.173.39	147.237.77.216		dover.idf.il	Tehila - Perl LWP with fake user agent	1
85.64.226.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.240.236.119	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
223.151.202.139	147.237.76.34	China	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.240.236.119	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
66.240.192.138	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	84
79.183.69.223	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
2.54.12.14	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
2.54.39.133	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
213.57.182.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
37.26.146.200	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
213.57.182.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.86.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.29.147	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.39.55.65	Russian Federation	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	illegal header format detected: Malformed HTTP format in request	monitor	6
46.19.85.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.120.125.22		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.148.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.235.79.47	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
77.127.229.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.154.65	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.102.254.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.228.46.121	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.253.59	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.47.254	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
109.253.133.180	Israel	147.237.72.167	ishurim.aka.idf.i	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
94.230.86.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.168.195.218	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
176.13.5.118	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
2.52.14.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.181.146.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.65.15.120	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
188.120.148.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.71	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.179.228.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.198	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.235.79.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.152.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.121	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.127.153.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.146.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.253.72	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.131.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.27.105.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
105.199.255.36	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
46.19.86.229	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.66.174.84	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
176.13.15.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
46.19.85.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
5.22.131.121	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	44
2.54.177.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.13.11.40	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.11.40	None	11
176.13.20.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.179.228.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.210.187.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.141.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.10.19	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
109.66.80.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.57.182.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.67.6.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.150.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.109.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.5.118	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
2.54.8.193	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/meretz	Block	1
212.76.110.38	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/haredim/contactus.aspx	None	1
79.178.10.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
160.176.173.39		147.237.77.216	dover.idf.il	Admin Blocking	Block	1
46.120.60.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.252.56	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH)	None	1
185.100.85.191		147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
93.172.166.240	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
176.13.10.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.64.87	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
109.253.196.177	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.118.144	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
212.235.79.47	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
180.76.15.135	China	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
160.176.173.39		147.237.77.216	dover.idf.il	PHP Attempt	Block	1
46.120.236.181	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 46.120.236.181	Block	1
109.160.207.194	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
93.173.5.114	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
176.13.11.40	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
37.142.64.87	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
109.253.198.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
2.54.29.147	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.25.151.159	Poland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
79.182.148.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
160.176.173.39		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-admin/admin-ajax.php	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
5.29.87.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
109.253.138.13	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1