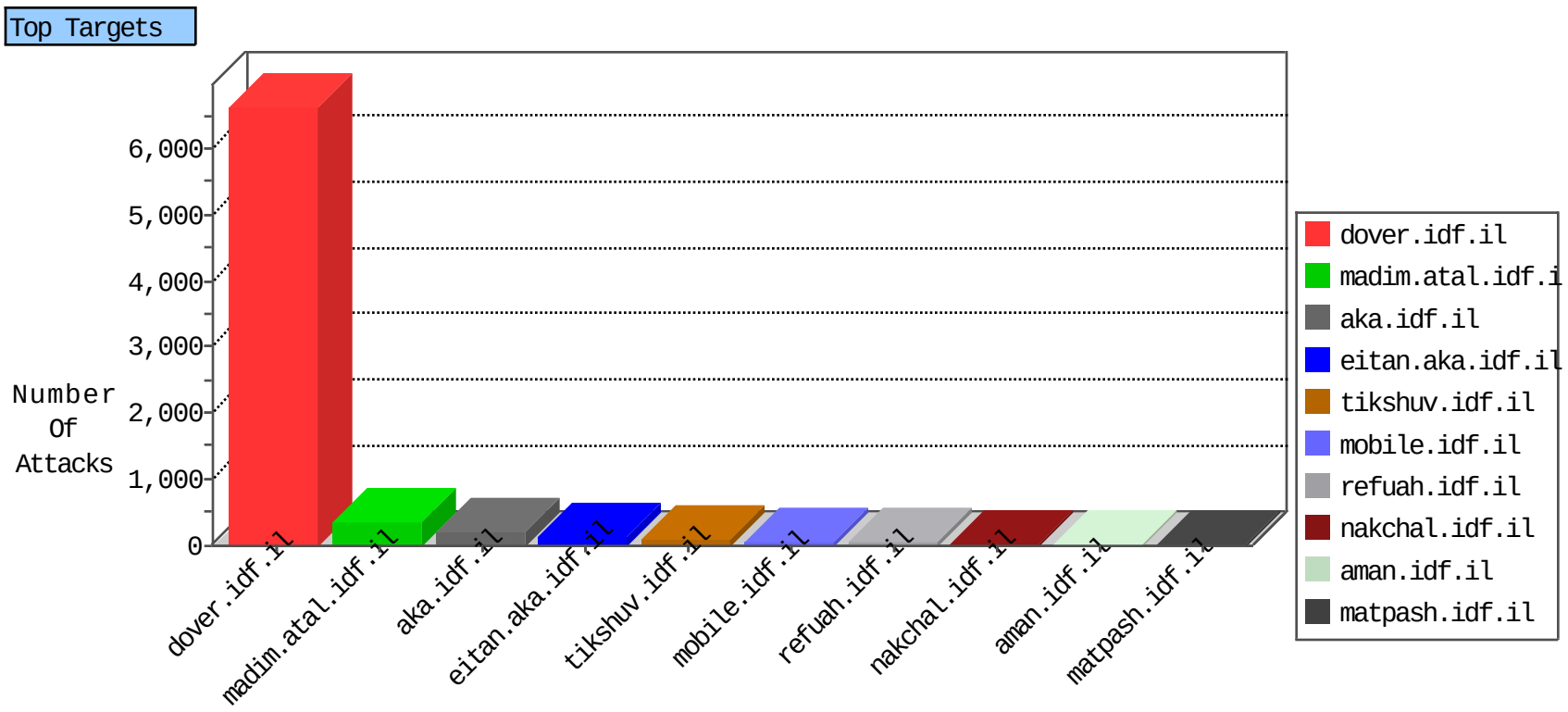
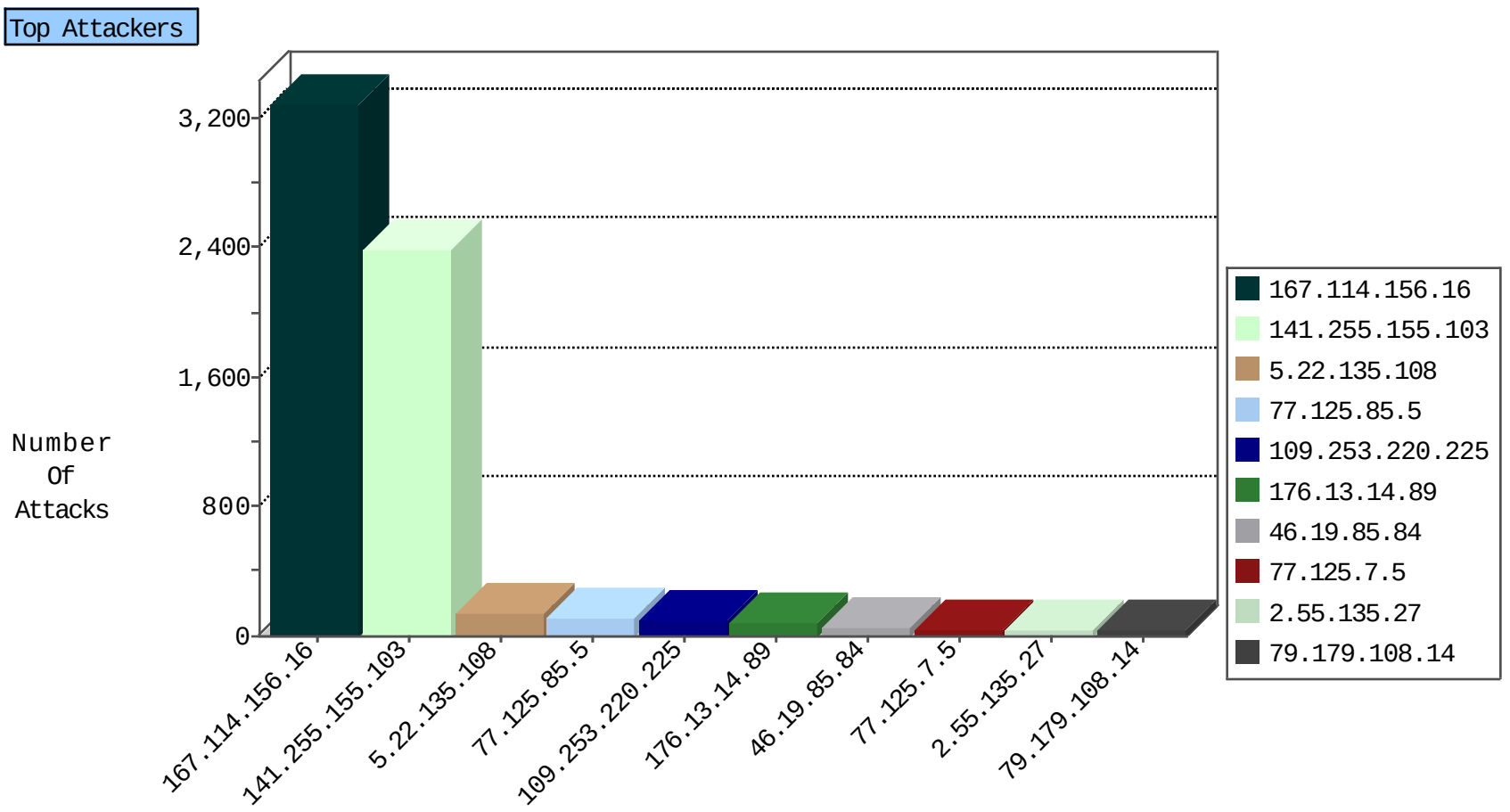
04-13-2016-17:04:04 to 04-13-2016-18:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-13-2016-17:04:04 to 04-13-2016-18:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.255.155.103	Netherlands	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	120627
141.255.155.103	Netherlands	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	8368
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3282
141.255.155.103	Netherlands	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	956
79.183.32.243	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
79.183.32.243	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.56.125	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1
2.53.25.51	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
81.218.56.125	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

04-13-2016-17:04:04 to 04-13-2016-18:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.127.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
84.108.163.118	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
82.81.76.144	Israel	147.237.77.170	maarachot.idf.il	C1000008: HTTP: Xenu UserAgent	Block	3
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
101.99.64.59	Malaysia	147.237.72.166	aka.idf.il	C1000016: HTTP: administrator in URI	Block	1

04-13-2016-17:04:04 to 04-13-2016-18:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
207.232.46.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.50.5.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.101.229	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
75.151.108.30	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.26.149.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
101.99.64.59	147.237.72.166	Malaysia	aka.idf.il	SERVER-WEBAPP admin.php access	1
79.178.142.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.150.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-13-2016-17:04:04 to 04-13-2016-18:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.22.135.108	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	138
77.125.7.5	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
125.215.235.181	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
79.179.108.14	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
148.177.129.212	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
31.154.156.131	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
212.76.127.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
195.244.23.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
41.242.65.10	Nigeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
109.67.187.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
212.76.127.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
106.38.241.106	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
149.78.82.129	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
62.219.21.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
77.171.50.176	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.186.49.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.147.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
87.70.48.137	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
79.178.5.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
213.6.119.94	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
149.50.27.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.65.97.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
197.45.132.217	Egypt	147.237.77.216	dover.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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.182.174.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
101.183.43.198	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.55.135.27	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
79.179.108.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.55.135.27	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	8
79.178.178.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.72	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
31.154.165.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.147.186	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
2.53.50.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.29.163.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
62.219.99.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
65.55.210.107	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.55.135.27	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

04-13-2016-17:04:04 to 04-13-2016-18:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.125.85.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
109.253.220.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
176.13.14.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
81.218.116.129	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	15
46.19.86.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
199.30.24.188	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
185.32.179.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.78.76.127	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.3.64	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	3
81.218.116.129	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	3
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.158.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtMobile in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	3
199.30.25.28	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.83.251	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.37	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.142.68.56	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
101.99.64.59	Malaysia	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
176.13.3.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.217	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
101.99.64.59	Malaysia	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 101.99.64.59	Block	2
176.13.4.140	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CaptchaText in mobile.idf.il/authentication/login	Block	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
89.139.162.57	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
2.53.40.43	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.221.69.168	Lithuania	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
173.88.166.253	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.69.19	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/scriptresource.axd	Block	1
104.236.96.48	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 104.236.96.48	Block	1
5.22.135.208	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 5.22.135.208	Block	1
101.99.64.59	Malaysia	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
2.53.135.214	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
77.221.69.168	Lithuania	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
207.241.229.149	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/sitemap/sitemap.aspx	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
104.236.96.48	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/14-he	Block	1
66.249.83.254	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
195.189.193.1	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
157.55.39.65	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.55.41.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.199.143.202	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
79.178.114.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ********** ********** ********** **********, Observed ********** ********** ********** ****	None	1
109.186.48.255	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
84.110.38.110	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb14662882 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
66.249.69.3	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/shared/clientscripts/clientscripts.js	Block	1
5.22.134.192	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

04-13-2016-17:04:04 to 04-13-2016-18:04:04