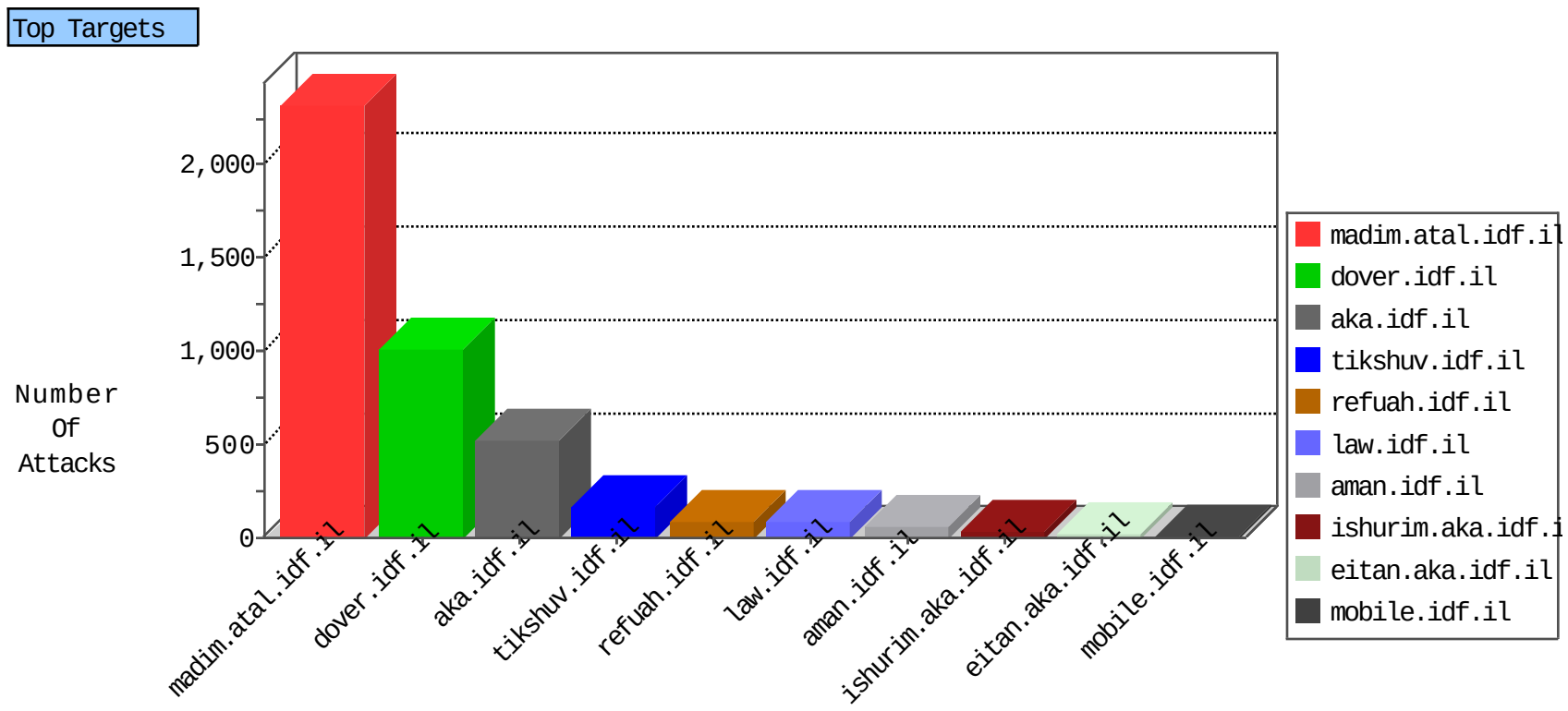
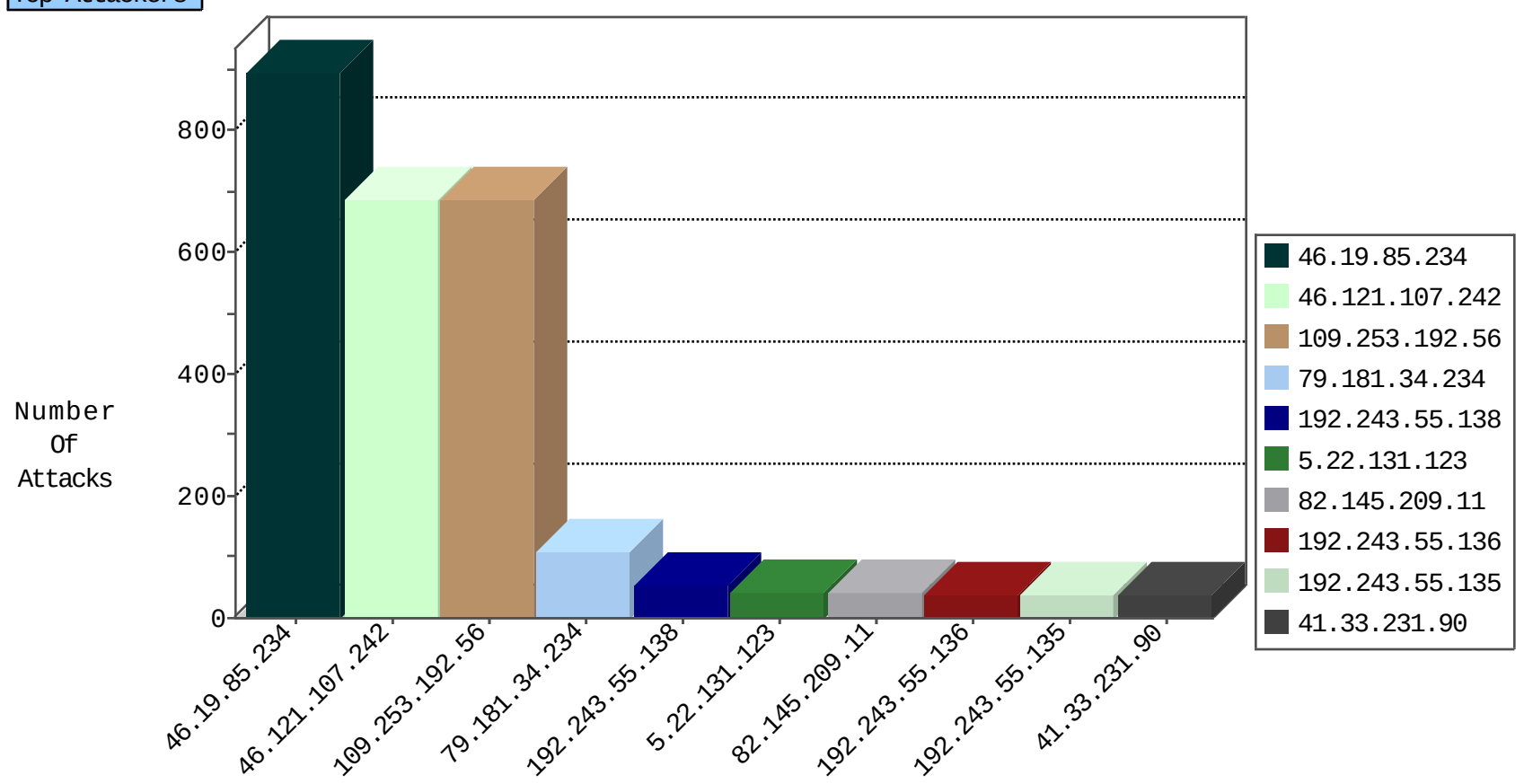
02-21-2016-20:04:07 to 02-21-2016-21:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-21-2016-20:04:07 to 02-21-2016-21:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.33	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	17
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.10	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	2
141.212.122.216	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
46.42.166.168	Russian Federation	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	1

02-21-2016-20:04:07 to 02-21-2016-21:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.211.235	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	16
106.120.173.109	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	8
149.88.143.84	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.180.241.238	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	6
84.228.197.36	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	6
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
89.216.115.6		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	1

02-21-2016-20:04:07 to 02-21-2016-21:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
79.178.201.20	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.212.119	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.69.143	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.177.215	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.172.96	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.242.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.139.162.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.67.1.109	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
5.22.131.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.59.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.37	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
189.202.241.84	147.237.8.27	Mexico	e.madim.atal.idf.i	ET SCAN NMAP -sS window 3072	1
80.178.24.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.82.106.200	147.237.76.202	India	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.56.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.213.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.179.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.222.121.61	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.80.224	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
14.199.145.126	147.237.76.30	Hong Kong	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
95.84.240.160	147.237.76.201	Russian Federation	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.119.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.252.23	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.67.1.109	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
84.94.180.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
189.202.241.84	147.237.8.27	Mexico	e.madim.atal.idf.i	ET SCAN NMAP -sS window 4096	1
80.246.136.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.103.252.2	147.237.72.156		aman.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.129.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.6.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-21-2016-20:04:07 to 02-21-2016-21:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.145.209.11	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	40
5.22.131.123	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	33
46.42.166.168	Russian Federation	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
178.27.200.203	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	24
79.180.215.227	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	20
109.253.150.70	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
141.8.132.2	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
5.102.242.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
5.255.253.10	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
213.57.247.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.23.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
46.19.85.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.19.85.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.85.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.66.10.29	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.216	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
94.230.86.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.179.214.113	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.179.214.113	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.46.38.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.55	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

02-21-2016-20:04:07 to 02-21-2016-21:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	660
46.121.107.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	521
109.253.192.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	489
46.19.85.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	237
109.253.192.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	197
46.121.107.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	168
79.181.34.234	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.181.34.234	Block	107
77.125.115.24	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.125.115.24	Block	27
87.69.86.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.86.219	Block	10
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	10
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	10
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	9
66.249.81.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	9
46.19.85.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
109.64.9.110	Israel	147.237.76.31	nakchal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
85.250.136.247	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.250.136.247	Block	6
37.26.149.192	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
37.142.246.25	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.142.246.25	Block	6
168.63.200.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
5.28.181.241	Israel	147.237.0.19	madim.atal.idf.i	Multiple Unauthorized URL Access from 5.28.181.241	Block	6
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
68.197.228.235	United States	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
66.249.81.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
79.182.104.95	Israel	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
41.102.117.190	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	4
220.255.148.212	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
185.89.217.224		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
5.28.181.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed PHP Attempt	Block	4
85.250.136.247	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
37.142.246.25	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
185.32.179.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.149.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.211.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3
109.253.194.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
5.22.131.123	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	2
176.13.19.65	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
109.66.121.209	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	2
212.34.12.21	Jordan	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	2
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 217.194.198.104 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
5.22.129.96	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/113639.pdf	Block	2
176.13.7.9	Israel	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
109.65.141.242	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	2
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
31.168.76.22	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	2
87.71.35.57	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/6/size338x0/1796.jpg	Block	2

02-21-2016-20:04:07 to 02-21-2016-21:04:07