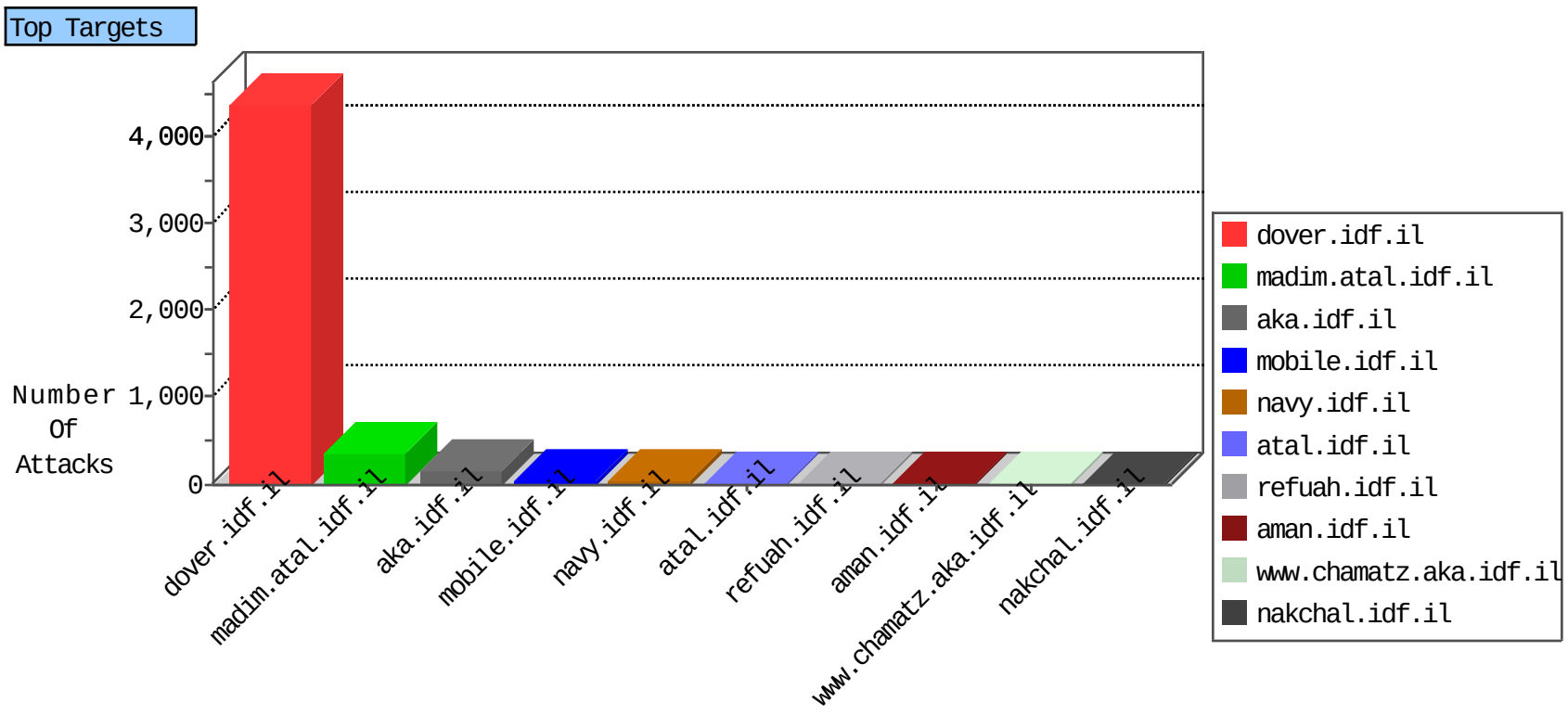
04-19-2016-15:04:09 to 04-19-2016-16:04:09

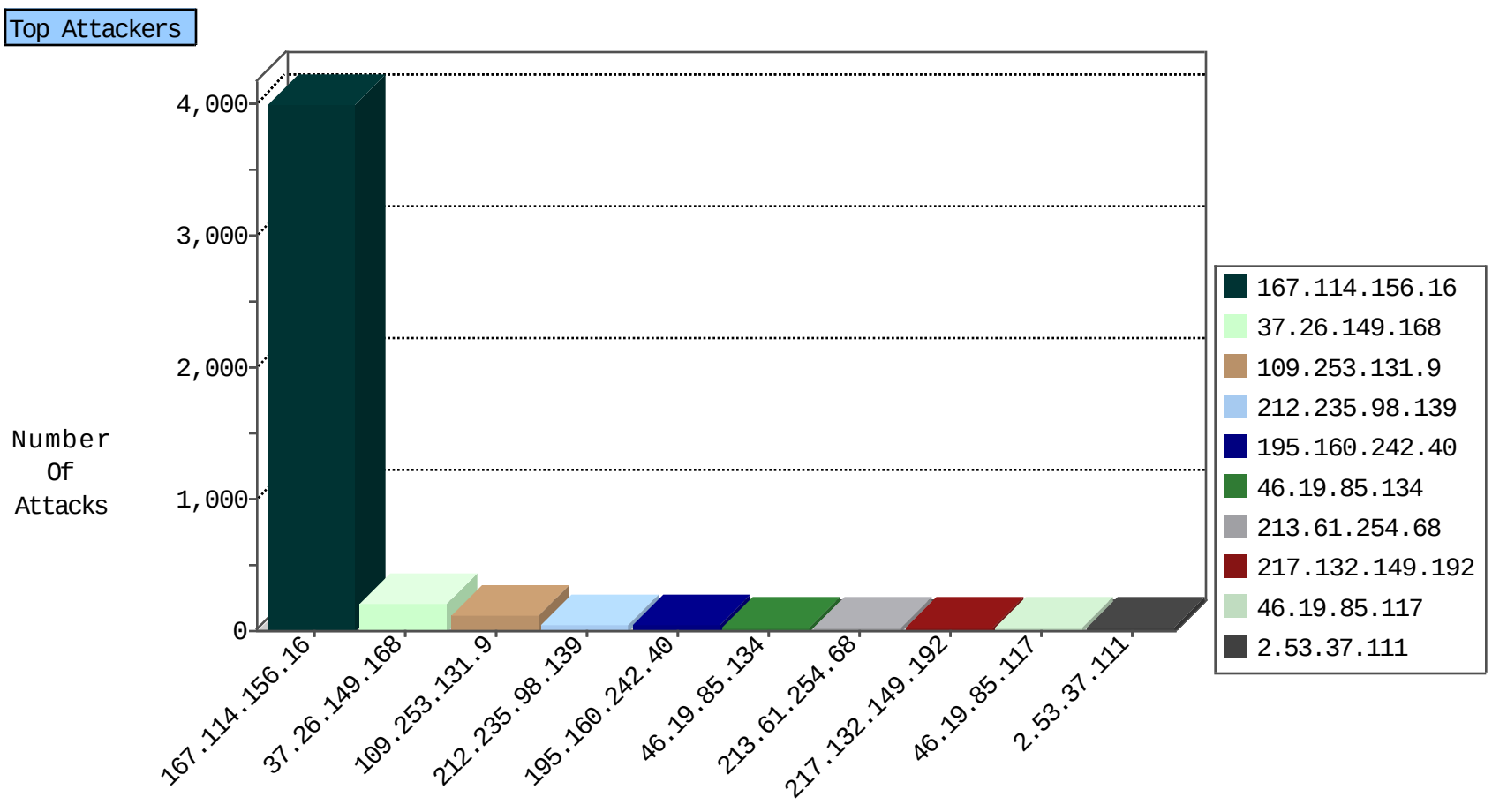
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-19-2016-15:04:09 to 04-19-2016-16:04:09

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	Block_Ip_Web_In	drop	4000
2.53.5.23	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2909
212.235.98.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
109.253.225.82	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
79.177.191.243	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.177.191.243	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
141.0.14.216	Europe	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
141.0.14.216	Europe	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	1
185.103.252.42	Russian Federation	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
69.30.221.42	United States	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
123.30.183.145	Vietnam	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
82.145.217.145	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	1
66.240.192.138	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
89.181.28.186	Portugal	147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	1
69.30.221.42	United States	147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	1

04-19-2016-15:04:09 to 04-19-2016-16:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.90.147.81	Sweden	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

04-19-2016-15:04:09 to 04-19-2016-16:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
93.90.147.81	147.237.77.233	Sweden	atal.idf.il	SQL Injection - Select From	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
80.178.99.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
190.124.35.115	147.237.76.39	Nicaragua	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
52.38.119.76	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 2048	1
132.64.30.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.125.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
122.141.236.69	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
31.168.0.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
114.33.31.132	147.237.0.19	Taiwan	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.53.156.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.155	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.169.192	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.93.241	147.237.77.176	Europe	matpash.idf.il	ET SCAN NMAP -sA (2)	1
194.90.121.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.237.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.18.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
52.38.119.76	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -f -sS	1
125.212.232.165	147.237.8.27	Vietnam	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.146.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
122.141.236.69	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
23.96.109.87	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
104.214.149.209	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 3072	1
2.53.155.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.155	147.237.76.196	Ukraine	e.sviva.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

04-19-2016-15:04:09 to 04-19-2016-16:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
213.61.254.68	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
217.132.149.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
213.151.55.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.37.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.134	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.134	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.117	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.137.82	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.55.8.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.117	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
213.61.254.67	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.246.139.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
89.139.163.122	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
37.26.149.198	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.148.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	6
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.235.98.139	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.160.242.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
209.173.241.141	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.22.131.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.177.171.40	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.148.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.177.171.40	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.30	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.54.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.253.202.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.117.49.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.0.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.213.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
132.66.152.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.110.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.8.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
165.225.72.81	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.235.43.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.168.113.35	United Kingdom	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
132.66.227.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-19-2016-15:04:09 to 04-19-2016-16:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	197
109.253.131.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
2.53.0.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
213.151.46.180	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 213.151.46.180	Block	9
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	8
2.53.37.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
85.250.4.143	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.250.4.143	Block	5
46.19.85.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.92.182.124		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.1.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.138.108.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.119.127.129	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.119.127.129	Block	3
213.151.46.180	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	3
37.26.147.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	2
37.26.148.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.37.111	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
220.255.148.148	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	2
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.147.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
169.229.3.91	United States	147.237.77.233	atal.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Illegal Byte Code Character in URL	Block	1
217.194.195.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
109.253.211.1	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
89.216.21.34		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
203.127.58.234	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.168.113.35	United Kingdom	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Malformed HTTP Header Line 1	Block	1
46.120.186.151	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
37.110.117.31	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
176.13.1.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Parameter Type Violation on madim.atal.idf.il/mobile/login.aspx parameter ctl00$ContentPlaceHolder1$txtCaptcha	Block	1
87.69.208.55	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.208.55	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
46.19.85.150	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/1919.jpg	Block	1
220.255.146.134	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.0.14.216	Europe	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	1
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-15198-	Block	1
203.127.96.244	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Distributed Abnormally Long Request	Block	1
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Malformed URL	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
37.187.56.76	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.187.56.76	Block	1
213.61.254.67	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

04-19-2016-15:04:09 to 04-19-2016-16:04:09