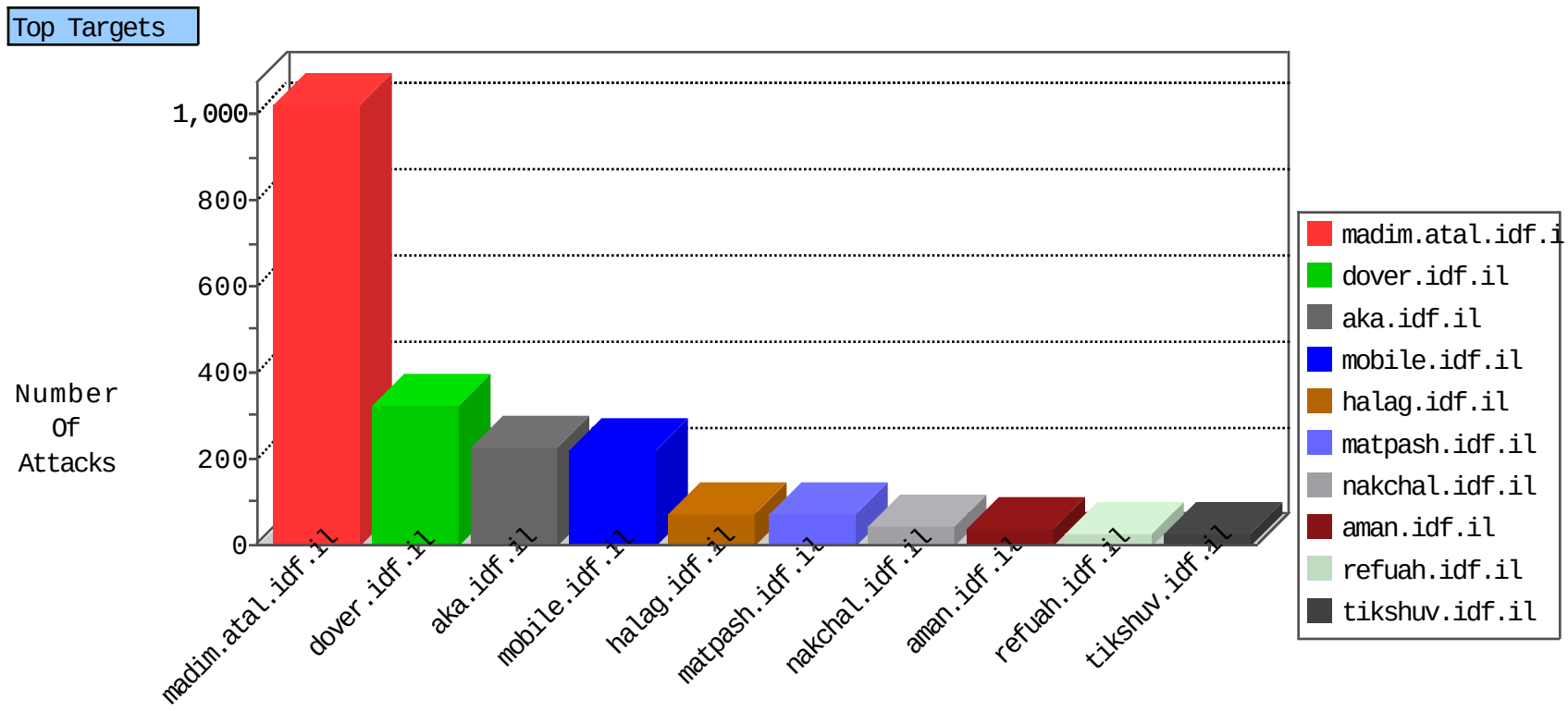
01-27-2016-20:04:02 to 01-27-2016-21:04:02

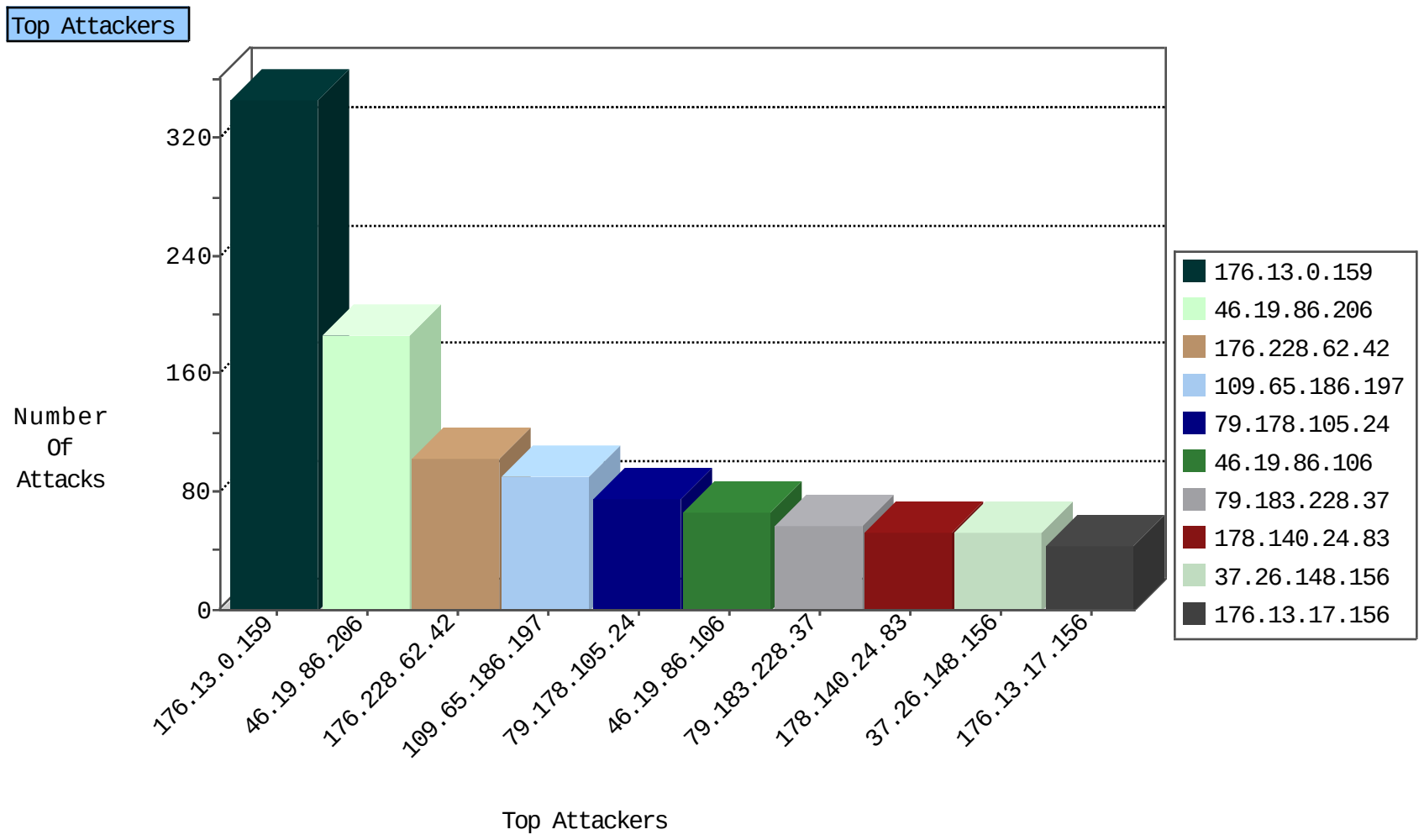
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-27-2016-20:04:02 to 01-27-2016-21:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	681
124.173.125.56	China	147.237.0.200	m4u.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
105.143.224.32	Morocco	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	2
111.50.67.74	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
54.67.38.74	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
105.158.219.212	Morocco	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
123.151.42.61	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
54.67.38.74	United States	147.237.77.19	law-forum.idf.il	DOS-httpdx-hreadrequest-FS	dest-reset	1
105.158.219.212	Morocco	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
105.158.219.212	Morocco	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

01-27-2016-20:04:02 to 01-27-2016-21:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.114	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

01-27-2016-20:04:02 to 01-27-2016-21:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.204.101.24	147.237.77.233	Lebanon	atal.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
105.143.224.32	147.237.76.38	Morocco	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
94.76.15.100	147.237.0.17	Bahrain	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.14.140	147.237.0.17	Bahrain	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
82.145.33.11	147.237.72.167	United Kingdom	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.152.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.228.136.107	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.206.237	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
105.143.224.32	147.237.76.38	Morocco	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
105.143.224.32	147.237.76.31	Morocco	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.14.140	147.237.0.33	Bahrain	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.76.1.202	147.237.0.16	Bahrain	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.161.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.133.183.106	147.237.8.27	Taiwan	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.26.146.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
1.164.197.19	147.237.76.30	Taiwan	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
168.62.238.153	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.67.41.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-27-2016-20:04:02 to 01-27-2016-21:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.183.228.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
178.140.24.83	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	41
109.186.8.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
176.13.17.156	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
79.182.204.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
37.142.177.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.155	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
209.140.32.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
37.26.146.170	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
37.26.146.170	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	19
212.179.229.81	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
176.13.4.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
213.204.101.24	Lebanon	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
213.204.101.24	Lebanon	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	13
37.26.146.158	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
77.126.229.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
93.173.241.36	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
37.26.146.158	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	7
46.19.86.84	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
94.230.86.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.166.57	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
84.95.3.99	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.177.10.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.13.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.85	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.76.127.10	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
94.230.86.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.191.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
94.230.86.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.241.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.250.232.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.202.104	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.22.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
188.120.148.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.68.21.145	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.0.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	176
176.13.0.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	158
46.19.86.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	106
176.228.62.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	103
109.65.186.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	83
46.19.86.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	81
79.178.105.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	75
46.19.86.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
37.26.148.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
109.253.131.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
185.32.179.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
37.142.68.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
5.29.72.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
176.13.0.159	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.0.159	Block	13
109.64.225.194	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 109.64.225.194	Block	12
79.183.228.37	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	12
37.142.177.111	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
176.13.17.156	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
176.13.17.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.65.186.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	6
84.228.38.148	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
79.182.204.134	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
79.179.29.209	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	4
79.178.24.205	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
5.29.198.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.130.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.148.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.4.103	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.178.24.205	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	3
2.52.137.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.148.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.29.171.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.160.244.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.202.104	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
41.238.49.79	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
2.54.191.64	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
213.151.50.35	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	2
46.120.101.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Unauthorized URL Access on madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
41.238.49.79	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	2
37.142.240.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.29.199.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.22.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.230.15.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.109.202.213	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/×″×?×ª×¨	Block	2
176.97.116.171	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
109.253.131.252	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
107.182.20.202	United States	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
66.249.78.140	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.78.140	Block	1

01-27-2016-20:04:02 to 01-27-2016-21:04:02