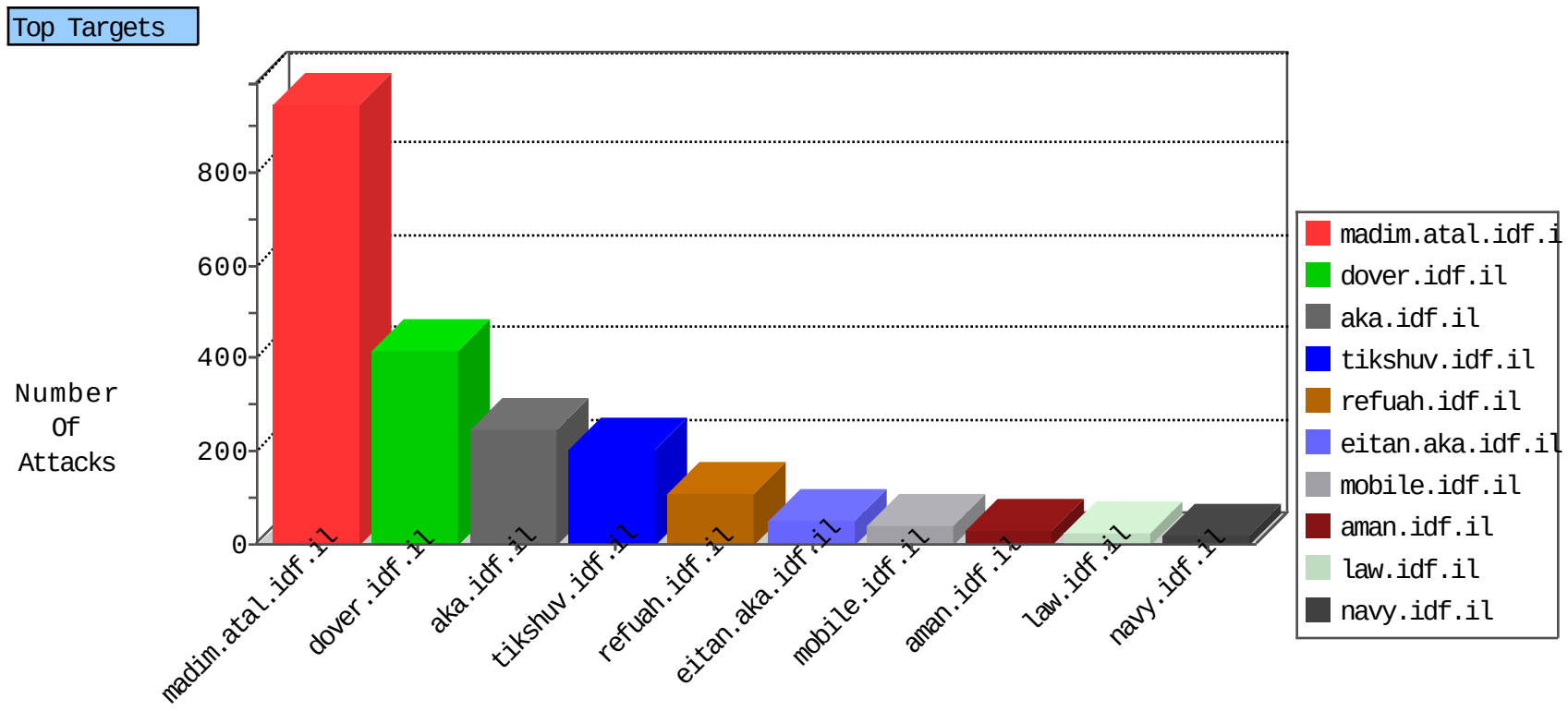
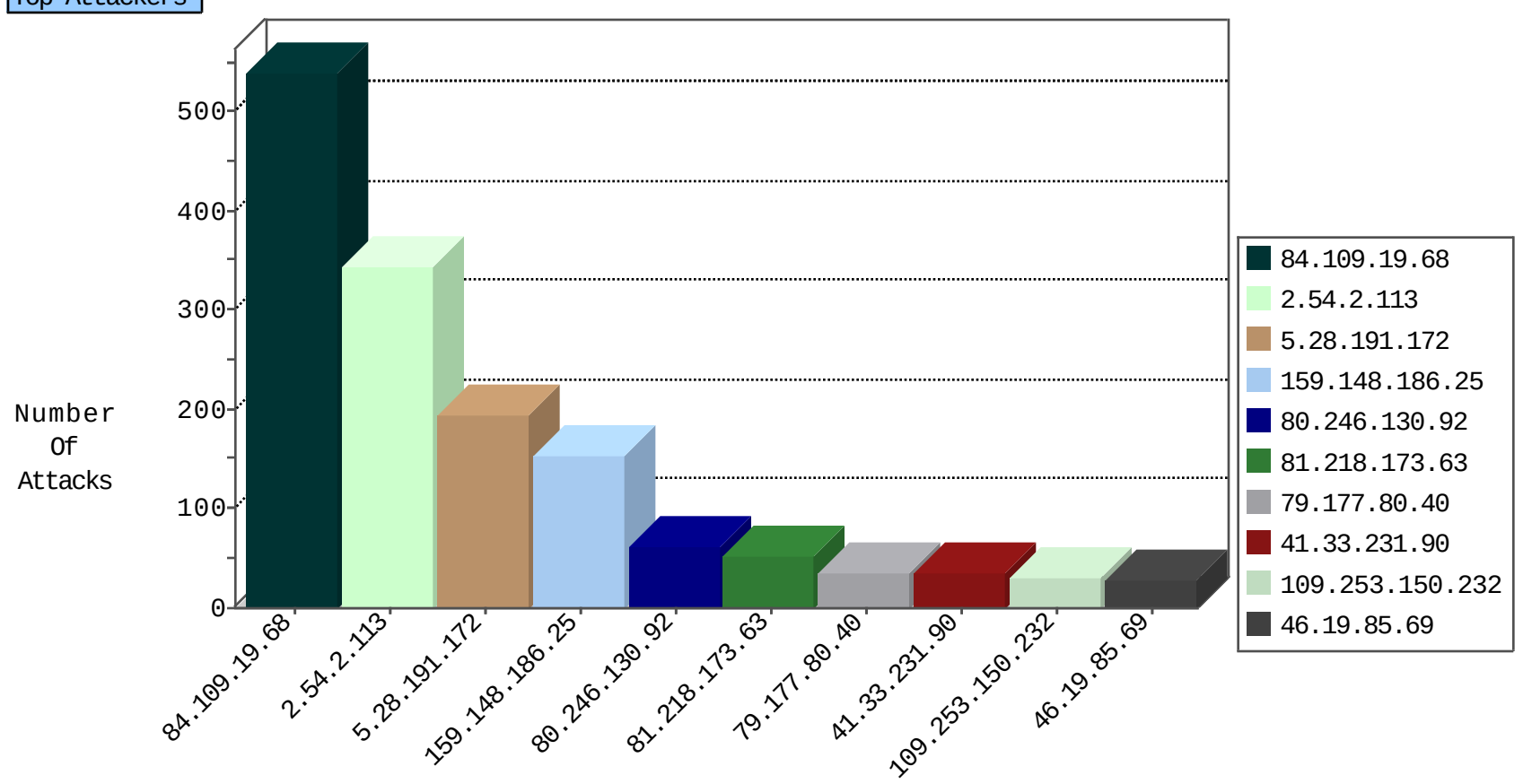
02-17-2016-19:04:02 to 02-17-2016-20:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-17-2016-19:04:02 to 02-17-2016-20:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
159.148.186.25	Latvia	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1004
159.148.186.25	Latvia	147.237.77.216	dover.idf.il	HTTP-MISC-Slow-HTTP-Test-DoS	source-reset	143
159.148.186.25	Latvia	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
24.78.209.175	Canada	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
198.58.103.160	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
45.35.64.142		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2

02-17-2016-19:04:02 to 02-17-2016-20:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-17-2016-19:04:02 to 02-17-2016-20:04:02

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	4
149.78.41.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.23.112.119	147.237.77.233	United States	atal.idf.il	ET SCAN Potential SSH Scan	1
93.173.155.85	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.23.112.119	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential SSH Scan	1
84.111.7.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.23.112.119	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
80.95.223.163	147.237.76.30	Bahrain	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.23.112.119	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
41.140.253.9	147.237.77.233	Morocco	atal.idf.il	ET SCAN NMAP -sS window 3072	1
190.216.146.151	147.237.0.34	Chile	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.201.61.82	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
2.54.189.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
188.64.169.106	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.201.61.82	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
212.16.78.12	147.237.76.42	Iran, Islamic Republic of	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
173.214.169.188	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
198.23.112.119	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential SSH Scan	1
109.66.58.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.23.112.119	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
93.113.125.11	147.237.76.196	Romania	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
198.23.112.119	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
84.108.207.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.23.112.119	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
46.116.217.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.68.193.231	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP admin.php access	1
190.216.146.151	147.237.0.33	Chile	idf.il	ET SCAN Potential SSH Scan	1
218.201.61.82	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
188.64.169.106	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
212.16.78.12	147.237.76.42	Iran, Islamic Republic of	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
173.214.169.188	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
212.16.78.12	147.237.76.42	Iran, Islamic Republic of	refuah.idf.il	ET SCAN NMAP -f -sS	1

02-17-2016-19:04:02 to 02-17-2016-20:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
159.148.186.25	Latvia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	102
80.246.130.92	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	60
79.177.80.40	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
81.218.173.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
82.145.208.200	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
176.13.8.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
81.218.173.63	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.69	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
217.194.194.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.85.69	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
84.108.244.47	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
149.101.1.118	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
37.26.148.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.76.127.219	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.64.37.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.156	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
5.102.242.182	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.29.225.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.251	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.214.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.2.113	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.85.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.46.41.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.148.137	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.2.113	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
185.120.126.35		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.185.253	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
146.185.56.182	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.102.254.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.199.7	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
84.109.19.68	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
217.194.194.217	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
41.209.66.199	Sudan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
212.76.127.44	Israel	147.237.0.34	tikshuv.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
109.67.200.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.212.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.199.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.94.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.163.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-17-2016-19:04:02 to 02-17-2016-20:04:02

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
5.43.210.193	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3

02-17-2016-19:04:02 to 02-17-2016-20:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.109.19.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	280
5.28.191.172	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 5.28.191.172	Block	194
2.54.2.113	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.2.113	Block	181
84.109.19.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	134
2.54.2.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
84.109.19.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	121
109.253.150.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
109.253.211.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
2.54.2.113	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.2.113	Block	19
109.66.58.61	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.66.58.61	Block	8
46.121.201.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
157.55.39.94	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.69	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	3
168.63.139.43	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
37.26.147.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
41.68.193.231	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
84.108.186.33	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	2
199.30.24.102	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
41.68.193.231	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.68.193.231	Block	2
217.194.194.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.180.99.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
197.38.197.170	Egypt	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	2
199.30.25.160	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.110.83.185	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
84.108.186.33	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
46.19.85.251	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
197.38.197.170	Egypt	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
84.108.186.33	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
77.126.117.60	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
5.28.191.172	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-10039-en	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3238.jpg	Block	1
213.57.226.144	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCity in madim.atal.idf.il/1088-he/meretz.aspx	Block	1
84.110.83.185	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
41.235.245.131	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
197.36.250.183	Egypt	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
37.26.149.180	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
80.246.130.92	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
5.22.135.153	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1
95.86.116.89	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/&sa=u&ved=0ahukewifomgcpf_kahxdkcwkhu4ldgkqfggimaa&usg=afqjcne4v5mzukzgf8eerlsefhnrvronew	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-en/dover.aspx	Block	1
46.19.86.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
197.38.197.170	Egypt	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
41.68.193.231	Egypt	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 41.68.193.231	Block	1
157.55.39.226	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/Ã—â€˜Ã—Å¾Ã—â„¢Ã—â€œÃ—â€?	Block	1
84.108.186.33	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
79.178.16.189	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
2.54.33.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.110.83.185	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1

02-17-2016-19:04:02 to 02-17-2016-20:04:02