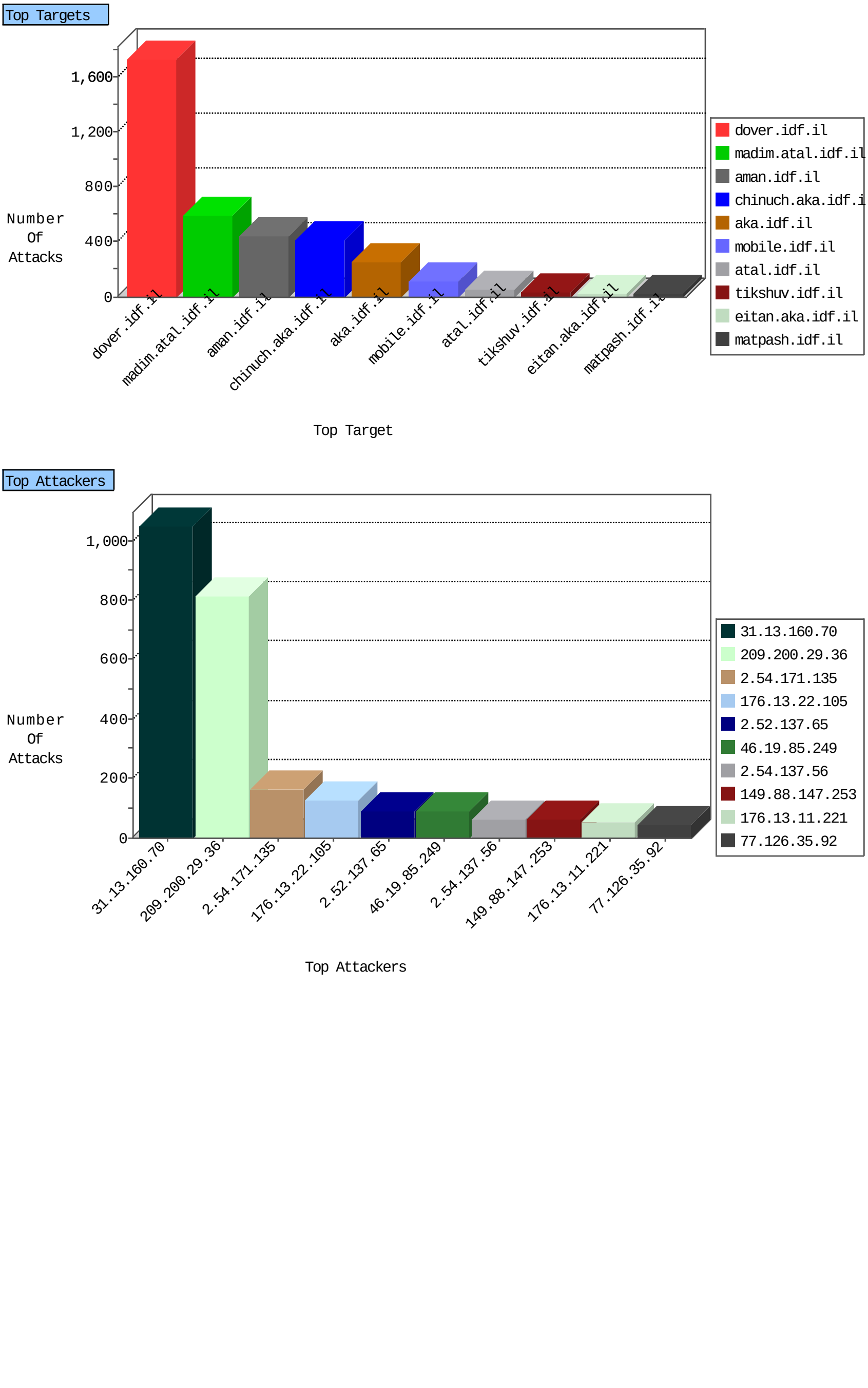
01-27-2016-19:04:07 to 01-27-2016-20:04:07

IDF Under Attack Daily Report



01-27-2016-19:04:07 to 01-27-2016-20:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.13.160.70	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP-MISC-Havij-User-Agent	dest-reset	2
54.67.38.74	United States	147.237.77.216	dover.idf.il	DOS-httpdx-hreadrequest-FS	dest-reset	1

01-27-2016-19:04:07 to 01-27-2016-20:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-27-2016-19:04:07 to 01-27-2016-20:04:07

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	4
218.246.0.97	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.128.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.153	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.197.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.249.14	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
98.231.219.210	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
36.72.228.72	147.237.77.205	Indonesia	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
94.76.14.140	147.237.76.30	Bahrain	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.29.181.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.76.14.140	147.237.0.17	Bahrain	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.76.14.140	147.237.0.15	Bahrain	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.250.87.193	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.242.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.191.117.60	147.237.72.166	Costa Rica	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.144.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
163.172.13.173	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.182.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
105.97.204.77	147.237.77.216	Algeria	dover.idf.il	SQL Injection - Select From	1
46.19.86.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.76.14.140	147.237.76.39	Bahrain	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
36.72.228.72	147.237.77.205	Indonesia	prisha.idf.il	ET SCAN NMAP -f -sS	1
94.76.14.140	147.237.0.34	Bahrain	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
5.29.14.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.76.14.140	147.237.0.17	Bahrain	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
89.139.165.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.141.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-27-2016-19:04:07 to 01-27-2016-20:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.13.160.70	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	532
31.13.160.70	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	516
209.200.29.36	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	407
209.200.29.36	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	406
2.54.171.135	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	136
2.54.137.56	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	62
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
79.178.34.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
149.78.111.233	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
176.13.18.164	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
93.172.8.118	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
89.138.89.166	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
141.0.14.217	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	16
109.253.198.30	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.2.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
77.126.24.178	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.19.85.105	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
2.54.60.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.177.181	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
46.19.86.153	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.209	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
85.65.201.135	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
109.67.162.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
149.78.184.181	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
2.54.171.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.171.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
2.54.171.135	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.163.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.155.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
98.170.222.14	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

01-27-2016-19:04:07 to 01-27-2016-20:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.137.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
176.13.22.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
46.19.85.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
149.88.147.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
176.13.11.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
176.13.22.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
77.126.35.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
176.13.14.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
84.94.190.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
46.19.85.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
5.29.135.236	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 5.29.135.236	Block	12
37.26.146.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
37.142.215.95	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	9
46.19.86.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
93.172.8.118	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
84.94.190.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
176.13.18.164	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.202.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.2.243	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.145.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.8.95.205	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	3
80.178.157.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.198.30	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.65.186.197	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
77.126.87.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	2
79.176.36.9	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
37.26.148.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.60.132	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	2
2.54.136.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.145.6	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
37.142.222.84	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	2
109.65.186.197	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtFirstName in madim.atal.idf.il/1088-he/meretz.aspx	Block	2
91.200.12.139	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
46.19.86.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	2
79.98.107.90	Bulgaria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
37.26.146.170	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.140	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
2.54.31.255	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
85.93.91.84	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	1
46.19.85.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.22.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.111.233	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1

01-27-2016-19:04:07 to 01-27-2016-20:04:07