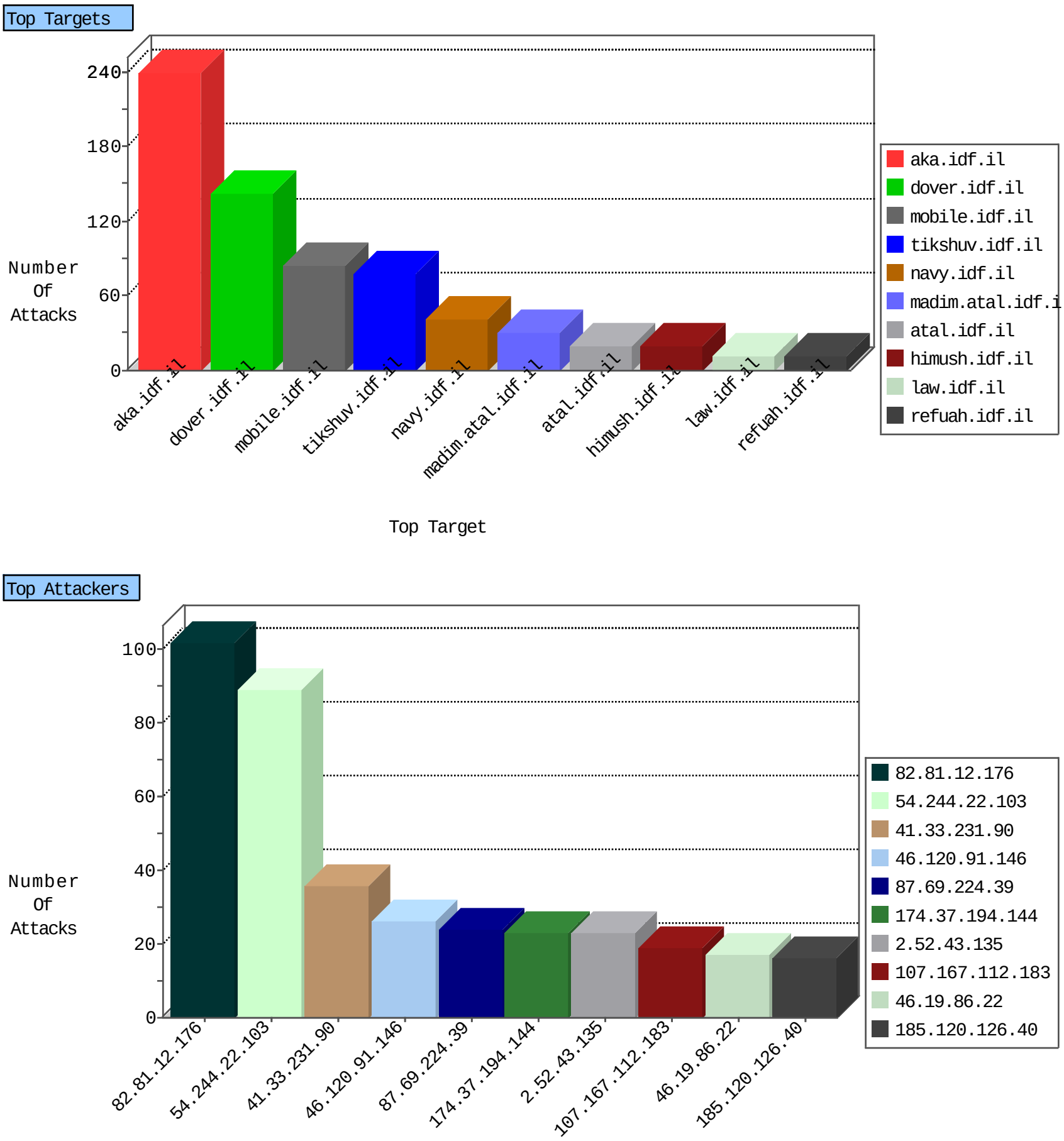
01-29-2016-21:04:09 to 01-29-2016-22:04:09

IDF Under Attack Daily Report



01-29-2016-21:04:09 to 01-29-2016-22:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	102
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
82.166.184.140	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
74.91.28.59	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	drop	1
217.146.91.36	United Kingdom	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

01-29-2016-21:04:09 to 01-29-2016-22:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-29-2016-21:04:09 to 01-29-2016-22:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
192.118.11.120	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
174.37.194.144	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
174.37.194.144	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
218.246.0.97	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
208.67.1.33	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
79.183.185.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.7	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
191.232.34.47	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
191.232.34.47	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
174.37.194.144	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
218.246.0.97	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
113.230.15.17	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
208.67.1.33	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
96.35.144.107	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
46.151.53.217	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
191.232.34.47	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
176.13.4.172	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

01-29-2016-21:04:09 to 01-29-2016-22:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	74
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.120.91.146	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
87.69.224.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
107.167.112.183	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
2.52.43.135	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
185.120.126.40		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	15
149.78.234.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
130.203.136.75	United States	147.237.77.74	law.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	8
37.46.39.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.4.172	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.4.172	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.126.165.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
174.37.194.144	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	4
46.120.144.85	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
174.37.194.144	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
80.246.133.42	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.12.83	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.182.62.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.247	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.67.137.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.235.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.120.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.138.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.125.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.132.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.13.61	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.254	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.46.44.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
52.33.66.29	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
188.120.148.139	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
89.139.152.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
213.57.159.246	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.86.44	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.65.114.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.67.96.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
174.37.194.144	United States	147.237.8.45	e.eitan.idf.il	drop	First packet isn't SYN	drop	2
213.57.159.246	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.129.216	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2

01-29-2016-21:04:09 to 01-29-2016-22:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.22	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.22	Block	14
31.154.94.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.64.41.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.52.43.135	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.13.4.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.22	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1540	Block	3
109.64.14.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.179.124.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.111.111.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.57.233.55	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files	Block	2
95.222.31.248	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.177.103.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
149.78.51.36	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
85.65.93.206	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	2
66.249.64.53	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/105632.pdf	Block	1
87.69.224.39	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sip_storage/files/	Block	1
84.109.214.228	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
188.143.232.22	Russian Federation	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1454-he/refuah.aspx	Block	1
76.188.81.87	United States	147.237.76.86	navy.idf.il	Unknown HTTP Request Method Â,[[#0]][[#0]][[#0]]t1EÂ?Â?8X_Â‹ccÃˆ ÂŒ^Ã›C>KÂ€(Ã•ÃžÂšÂ… in URL [[#29]]hdÂ¥	Block	1
149.78.120.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
76.188.81.87	United States	147.237.76.86	navy.idf.il	Abnormally Long Header Line request header name	Block	1
46.120.68.151	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/newsarchive.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
86.99.183.165	United Arab Emirates	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 86.99.183.165 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
31.13.102.109	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.133.42	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
76.188.81.87	United States	147.237.76.86	navy.idf.il	Illegal HTTP Version	Block	1
141.212.122.209	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
66.249.64.55	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
192.118.11.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
149.88.87.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.126.72.105	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
76.188.81.87	United States	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
65.208.151.113	United States	147.237.76.30	himush.idf.il	Multiple Unauthorized URL Access from 65.208.151.113	Block	1
86.99.183.165	United Arab Emirates	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
31.13.110.97	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/Ø§Ù^	Block	1
176.13.19.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.229.144.165	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
76.188.81.87	United States	147.237.76.86	navy.idf.il	Malformed URL [[#29]]hdÂ¥	Block	1
147.83.130.22	Spain	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
93.173.12.127	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb14154959 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.64.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/107201.pdf	Block	1
84.111.206.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
46.19.86.27	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	1
198.58.103.36	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
157.55.39.78	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1

01-29-2016-21:04:09 to 01-29-2016-22:04:09