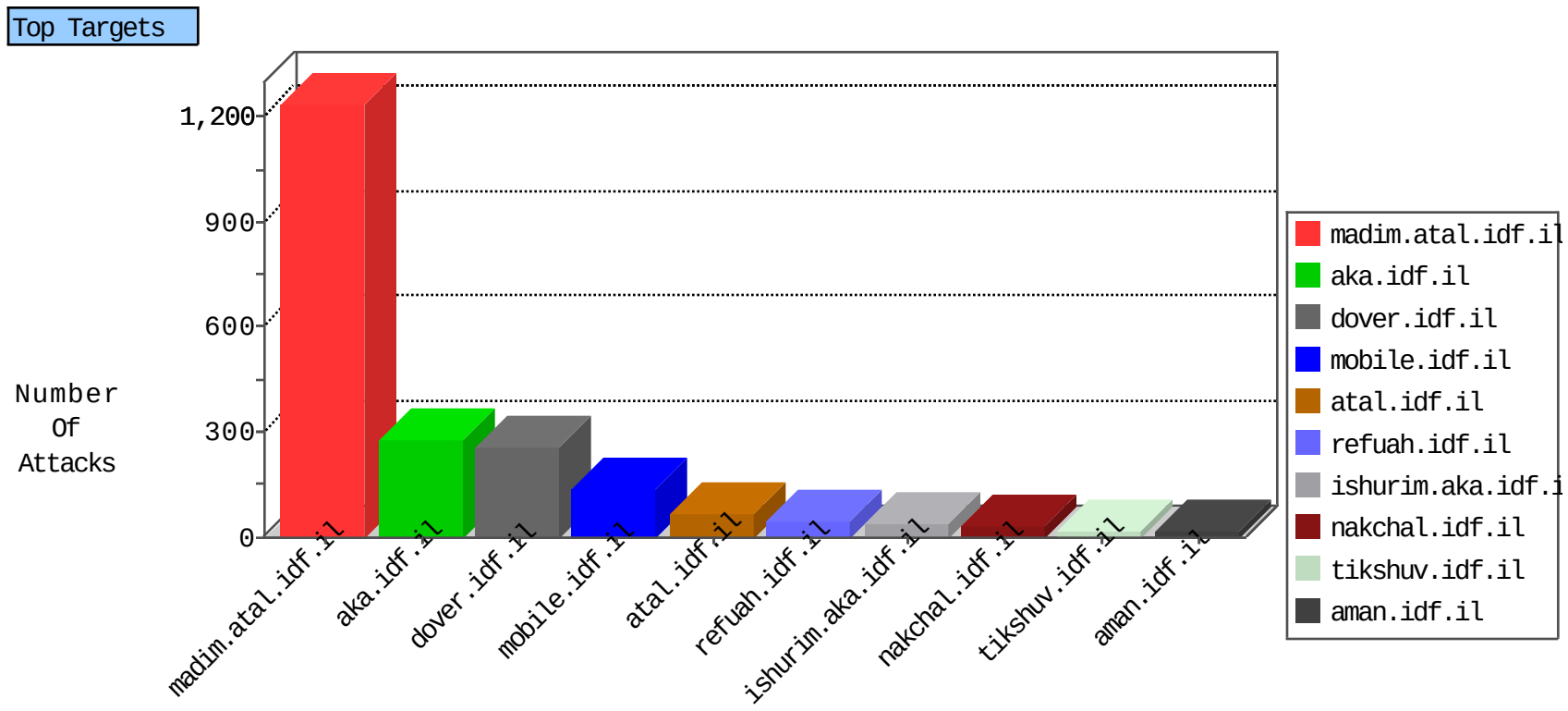
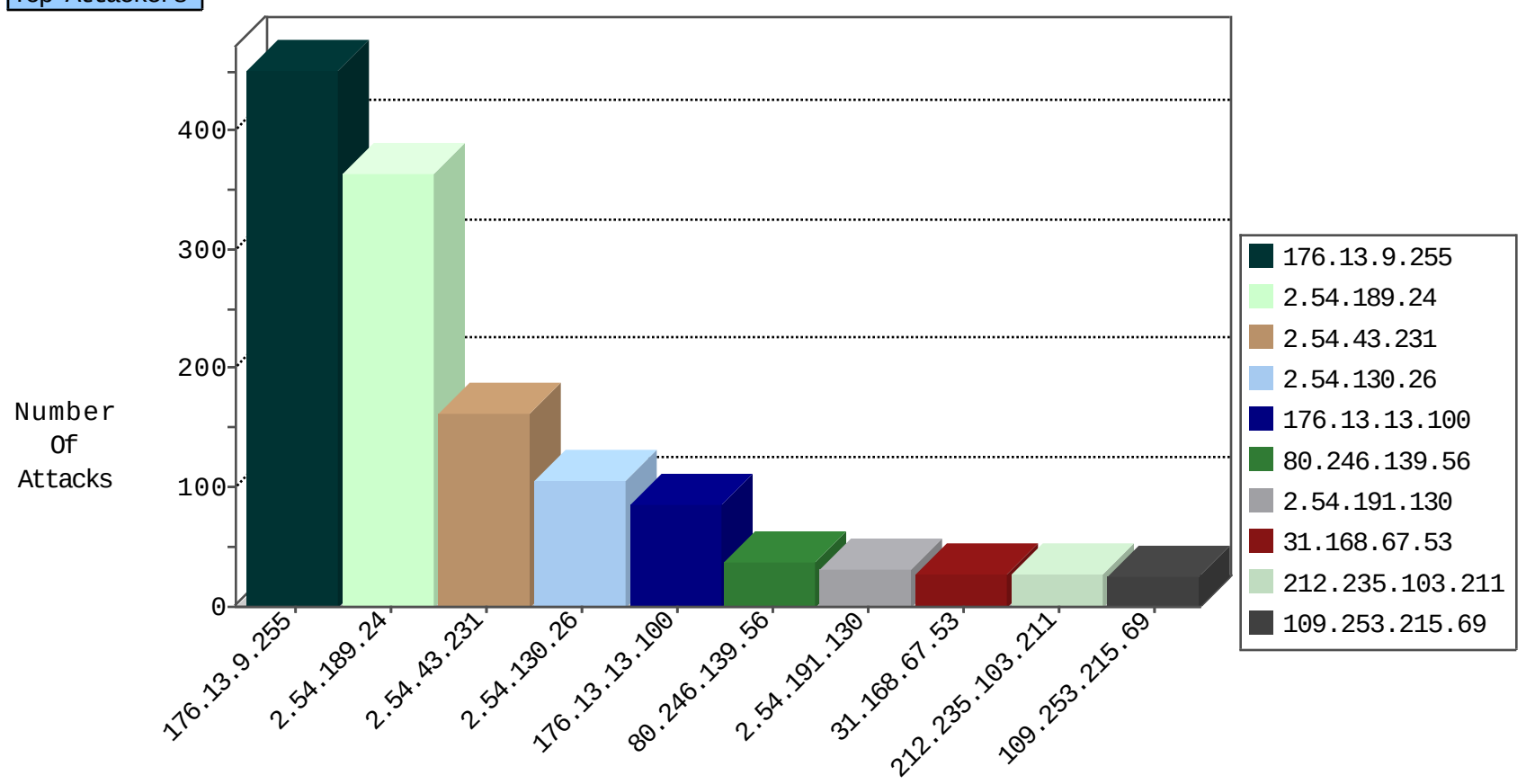
02-11-2016-13:04:08 to 02-11-2016-14:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-11-2016-13:04:08 to 02-11-2016-14:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.70.128.129	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
183.60.48.25	China	147.237.76.34	yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2

02-11-2016-13:04:08 to 02-11-2016-14:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
38.95.109.60	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
151.80.31.128	Italy	147.237.76.147	chinuch.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
38.95.109.60	United States	147.237.77.74	law.idf.il	C008: HTTP: Xenu UserAgent	Block	1

02-11-2016-13:04:08 to 02-11-2016-14:04:08

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	2
147.236.38.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
125.65.165.215	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
213.57.126.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.169.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.163.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.3.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.3.147.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.1.75.4	147.237.77.226	Australia	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
147.236.232.15	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.70.66.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
96.80.210.70	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.76.198	Ukraine	e.yohalan.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.25.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.12.82.58	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.19.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.117.188.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.19.236	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
168.1.75.4	147.237.8.27	Australia	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1

02-11-2016-13:04:08 to 02-11-2016-14:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.139.56	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
212.235.103.211	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	28
31.168.67.53	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
46.19.86.89	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
82.145.216.77	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
2.54.128.111	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
79.177.112.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
66.249.81.183	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	19
176.13.20.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
141.0.14.21	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
66.249.81.175	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	15
176.13.13.100	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
2.54.130.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.81.179	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	12
37.26.146.172	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
85.64.164.225	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
37.26.146.227	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.0.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.219.21.30	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.6.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.168.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.64.251.52	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
62.219.21.30	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
176.13.13.100	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
79.178.122.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.72.178	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
5.22.135.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.64.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.13.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
46.188.26.225	Russian Federation	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
147.236.34.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
147.236.34.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.164.244	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.160	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
117.222.136.43	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.93.182	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.47	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.117.136.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.229	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.130	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.201	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	4
79.181.49.31	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4

02-11-2016-13:04:08 to 02-11-2016-14:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.9.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	233
2.54.189.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	187
2.54.189.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
176.13.9.255	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.9.255	Block	110
176.13.9.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	109
2.54.130.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
2.54.43.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	82
2.54.43.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
2.54.189.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	68
176.13.13.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
2.54.191.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
109.253.215.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	13
80.246.139.56	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
2.54.170.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
62.219.21.30	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 62.219.21.30	Block	6
85.64.251.52	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	6
31.154.19.5	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	4
2.54.22.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.251.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.130.26	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.158.176	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
109.253.200.105	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtLastName	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
66.96.128.60	United States	147.237.72.156	aman.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	1
109.64.51.151	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$btnSend.x in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
2.54.1.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
46.19.86.89	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
78.154.160.245	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1395-en/dover.aspx	Block	1
31.154.41.13	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
147.236.238.55	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/3142.jpg	Block	1
2.54.46.113	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
89.247.108.58	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.116.93.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
46.19.85.48	Israel	147.237.76.31	nakchal.idf.il	Malformed URL	Block	1
79.181.217.210	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl79 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.78.239	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter lang in eitan.aka.idf.il/938-en/eitan.aspx	None	1
176.13.0.249	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
66.96.128.60	United States	147.237.72.156	aman.idf.il	Multiple signatures from 66.96.128.60	Block	1
46.19.86.109	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.176.64.152	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
31.168.67.53	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
205.139.141.54	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/iturim/asp/displayonesoldier.asp	None	1
157.55.39.28	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
62.219.21.30	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 62.219.21.30	Block	1
2.54.50.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

02-11-2016-13:04:08 to 02-11-2016-14:04:08