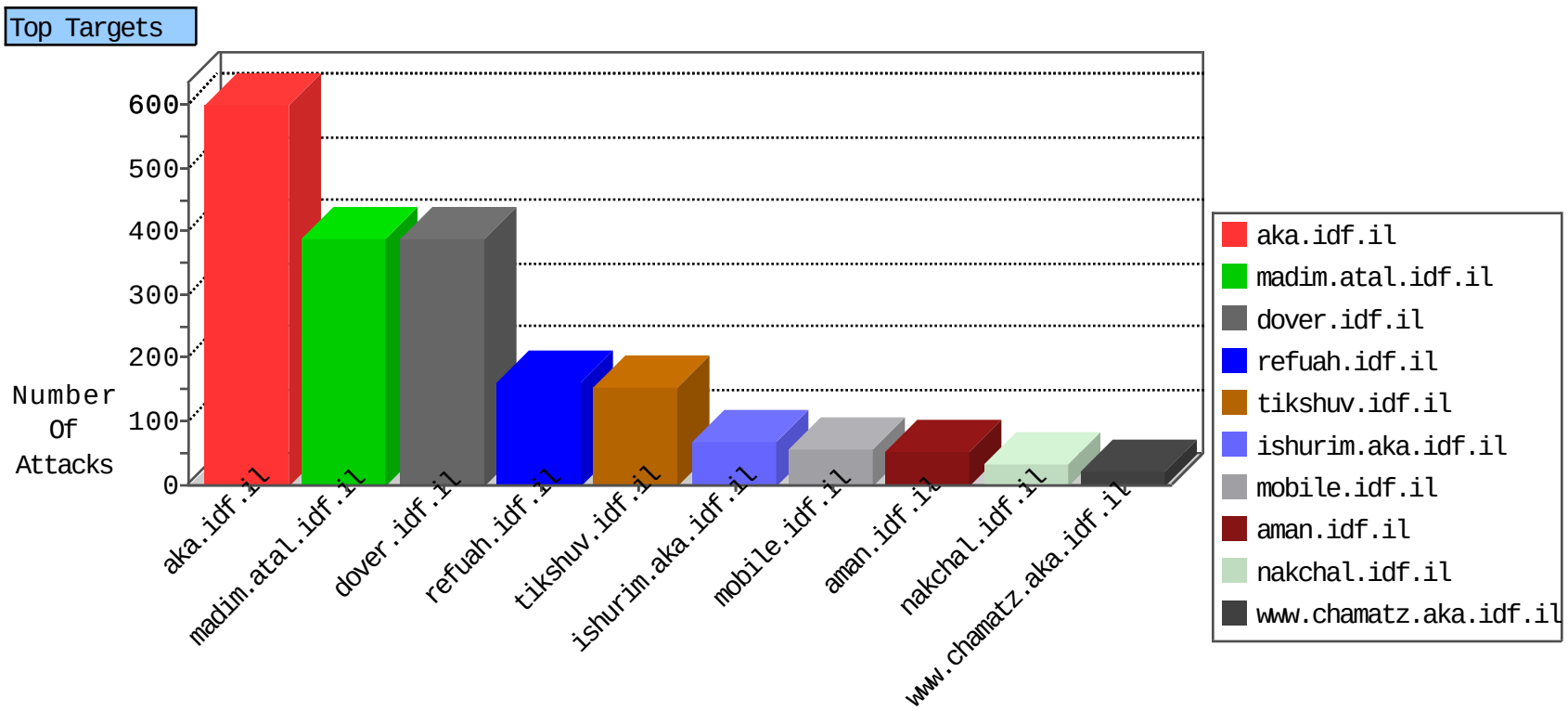
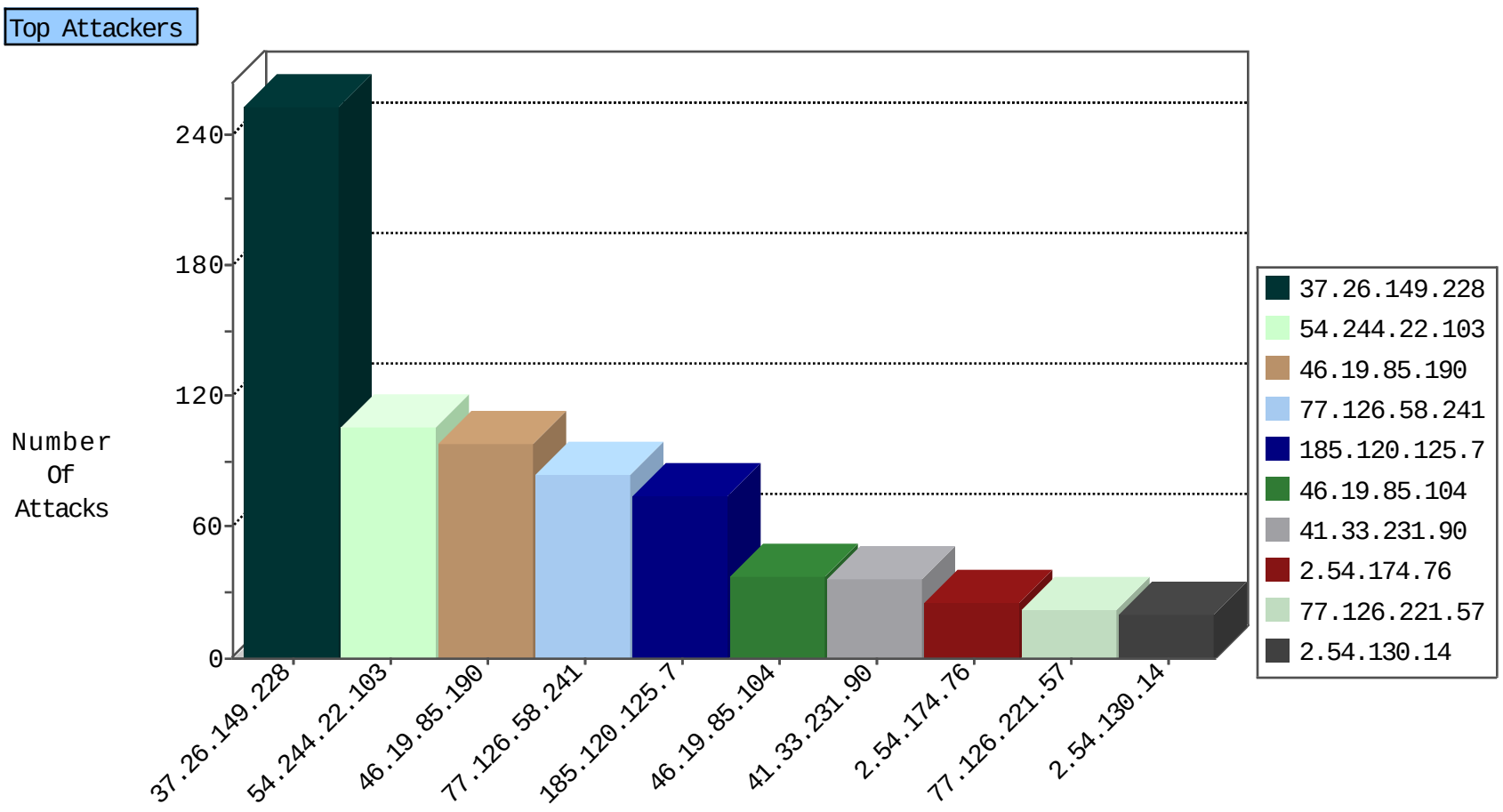
02-01-2016-16:04:08 to 02-01-2016-17:04:08

IDF Under Attack Daily Report



Top Target



Top Attackers

02-01-2016-16:04:08 to 02-01-2016-17:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	14
31.168.240.21	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
173.195.0.21	United States	147.237.0.34	tikshuv.idf.il	Invalid TCP Flags	drop	1
42.112.10.89	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
200.35.95.235	Venezuela	147.237.76.199	e.nakchal.idf.il	L4 Source or Dest Port Zero	drop	1
109.64.163.241	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid L4 Header Length	drop	1
42.112.10.85	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
173.195.0.22	United States	147.237.0.34	tikshuv.idf.il	Invalid TCP Flags	drop	1
42.112.10.92	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
142.54.169.164	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
42.112.10.87	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
173.195.0.23	United States	147.237.0.34	tikshuv.idf.il	Invalid TCP Flags	drop	1
42.112.10.93	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
42.112.10.65	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
142.54.169.164	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
42.112.10.88	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.130.5.174		147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
81.218.56.125	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1
42.112.10.66	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

02-01-2016-16:04:08 to 02-01-2016-17:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.116.50.134	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	4
192.116.50.134	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	4
212.179.225.88	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	2
192.116.50.134	Israel	147.237.76.86	navy.idf.il	C008: HTTP: Xenu UserAgent	Block	1
192.116.50.134	Israel	147.237.77.170	maarachot.idf.il	C008: HTTP: Xenu UserAgent	Block	1

02-01-2016-16:04:08 to 02-01-2016-17:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.180.150.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.8.14	Sweden	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
66.220.158.102	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
122.141.236.69	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
122.141.236.69	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.200.12.118	147.237.77.233	Ukraine	atal.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.164.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.117.113.152	147.237.77.226	Romania	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
82.118.226.189	147.237.72.156	Bulgaria	aman.idf.il	OS-OTHER Cisco IOS HTTP configuration attempt	1
80.246.136.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.237.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
79.177.138.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.155.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.122.189	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
122.141.236.69	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.249.174.151	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.61.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
84.109.96.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.60.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.118.226.189	147.237.72.156	Bulgaria	aman.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	1
79.181.217.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-01-2016-16:04:08 to 02-01-2016-17:04:08

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	99
77.126.58.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	69
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	50
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
77.126.221.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
185.89.217.233		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	19
80.246.133.65	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
176.12.154.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	17
185.89.217.230		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	13
212.235.103.211	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
185.89.217.229		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
46.19.85.104	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.104	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
185.89.217.224		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
185.89.217.234		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
46.121.120.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
206.41.88.154	Canada	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
2.54.174.76	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.1.255	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.174.76	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
185.89.217.227		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
2.54.130.14	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
62.219.224.145	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.85.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
185.89.217.231		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
185.89.217.232		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
185.89.217.228		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	7
5.22.131.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.148.201	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.46.39.92	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.177.201.131	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
185.32.179.28	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.177	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.48.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.46.20	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.89.217.225		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
37.26.148.240	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.181.169.114	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	6
79.177.201.131	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.89.217.235		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
132.66.40.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	127
37.26.149.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
46.19.85.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
79.180.101.206	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.180.101.206	Block	19
46.117.14.168	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	12
2.54.174.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
94.159.151.190	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 94.159.151.190	Block	9
80.179.143.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58339&docid=69689	Block	6
176.12.154.199	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	5
46.121.120.172	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.12.154.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.138.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.155.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.135.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.154.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
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
37.142.64.112	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
192.117.147.3	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
109.66.0.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mains/sachar	Block	2
2.54.1.255	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
95.86.99.61	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.99.61	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
79.179.166.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.227.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/&yoterws=1&yoter_user=2017	Block	2
188.120.135.179	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
62.0.103.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.120.245.159	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	2
79.179.99.48	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
46.19.86.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.5.14	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.81.244	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
185.49.14.190	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
79.182.187.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$3 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.121.102.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
146.185.234.48	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/news/news.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
77.126.58.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
77.126.58.241	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	1
5.29.6.190	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
95.86.99.61	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/	Block	1
176.12.155.187	Israel	147.237.72.166	aka.idf.il	Unknown Parameter _ in www.aka.idf.il/main/giyus/	None	1
79.179.119.125	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtLastName	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.i	Unknown HTTP Request Method M!Ã§Â¯Ã¯Ã¡yÃ?ÃŒÂ±ÃšÂ¿Â²Ãž [[#24]]P1}cÂ«Â-Â'HÂ? in URL	Block	1
77.126.58.241	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
212.143.111.30	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
31.168.116.1	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
89.139.136.160	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$1 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.81.247	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1