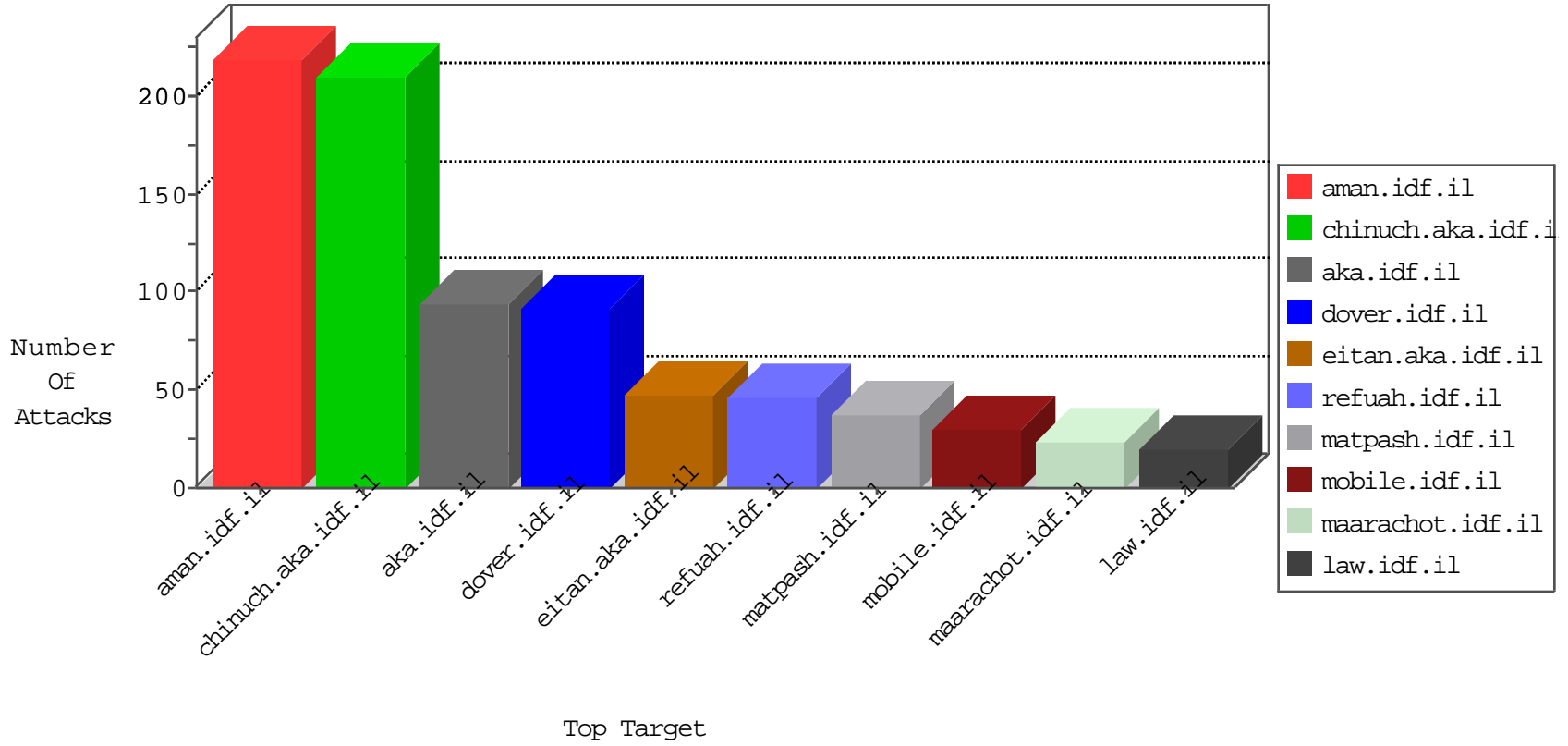


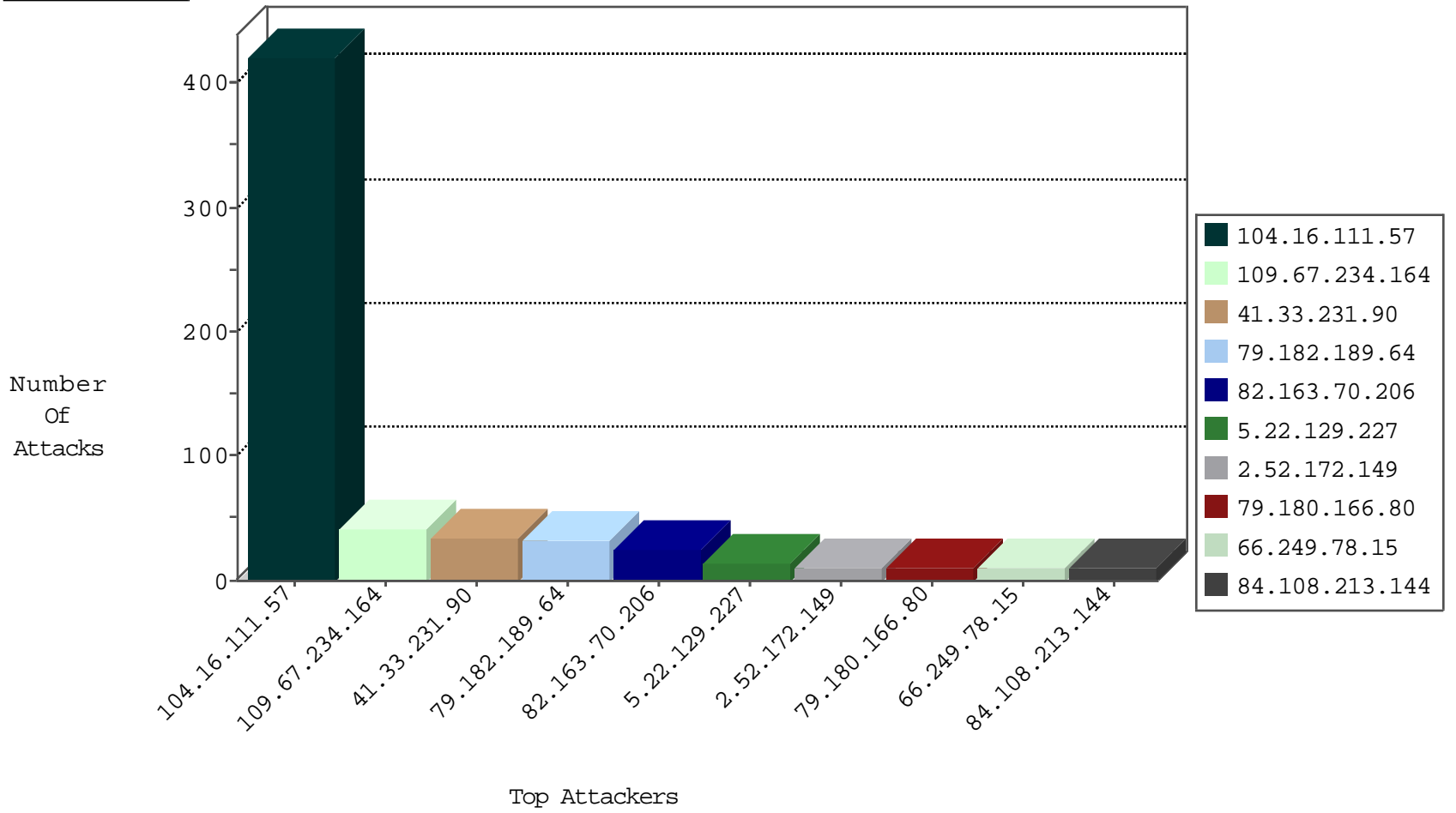
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
92.253.91.66	Jordan	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	633
82.163.70.206	United Kingdom	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	221
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	70
187.213.149.164	Mexico	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	50
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	26
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	25
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	10
134.147.203.115	Germany	147.237.76.38	e.e.meitav.idf.i	Block Ntp_All_Net	drop	2
123.151.149.222	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.63.97.227		147.237.76.42	refuah.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
45.63.97.227		147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
198.20.69.74	United States	147.237.76.201	e.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

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
66.249.81.198	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
186.210.198.88	147.237.8.27	Brazil	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.72.179.1	147.237.76.199		e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
180.113.114.22	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
114.112.90.54	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
88.150.252.21	147.237.0.33	United Kingdom	idf.il	ET SCAN Potential SSH Scan	1
62.8.68.118	147.237.76.31	Kenya	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.20.69.74	147.237.76.201	United States	e.atal.idf.il	ET DROP Dshield Block Listed Source	1
190.124.35.115	147.237.76.202	Nicaragua	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.1	147.237.76.199		e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.76.42	Austria	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
59.14.107.205	147.237.8.27	Korea, Republic of	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
209.126.116.147	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
104.16.111.57	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	208
104.16.111.57	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	208
109.67.234.164	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
79.182.189.64	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
79.182.189.64	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	15
5.22.129.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.172.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
87.69.178.112	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.213.144	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
199.30.25.67	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.59	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.129.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.67.167.16	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
78.40.181.35	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.117.143.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
79.180.166.80	Israel	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.120.202.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
84.108.213.144	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.66.113.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.54.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.14	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.66.169.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.226.51.15	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.162.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.145.95.42	United Kingdom	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.142.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.198	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.120.126.7		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.87.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.234.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
88.150.252.21	United Kingdom	147.237.0.33	idf.il	drop		drop	2
2.54.63.254	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.121.114.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.135.255	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.78.170	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.146.169	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence		alert	2
2.54.165.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.26.146.169	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence		monitor	2
109.253.147.21	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.81	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.43.203.182	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
95.218.133.253	Romania	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.14	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.166.80	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 79.180.166.80	Block	5
2.54.4.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.228.177.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	3
82.166.3.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.127.152.61	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
87.68.59.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.127.240.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	2
79.180.149.230	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$60 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	2
37.46.38.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.172.149	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	1
105.154.212.244	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
79.180.149.230	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$74 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/born2.htm	Block	1
175.44.8.45	China	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/chamatz/home/default.asp	None	1
40.77.167.94	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/news/www.sviva.gov.il	Block	1
197.116.53.62	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin	Block	1
54.197.157.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=62242&docid=76837	Block	1
109.67.167.16	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
68.180.229.31	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
46.19.85.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
65.132.59.34	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	1
109.186.180.137	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$83 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
31.13.110.105	Ireland	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/sip_storage/files/9/size220x0/2019.jpg	Block	1
79.180.166.80	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/113291	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakchal.idf.il/1100-he/nakchal.aspx	Block	1
185.65.252.128	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
46.117.143.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
87.69.178.112	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.180.149.230	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$42 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
198.58.99.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
66.249.65.152	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
109.253.220.173	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$42 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
31.210.188.29	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 31.210.188.29 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
79.182.189.64	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/3950.pdfxy-and-dirtyed-the-oklahoma-tornadows	Block	1
69.30.224.178	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
46.120.176.211	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$92 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
188.143.232.70	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$ucArticleLobbyControl\$datepicker in www.idf.il/1283-en/dover.aspx	Block	1
98.143.148.107	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/check	Block	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
128.138.65.205	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
80.246.136.59	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1