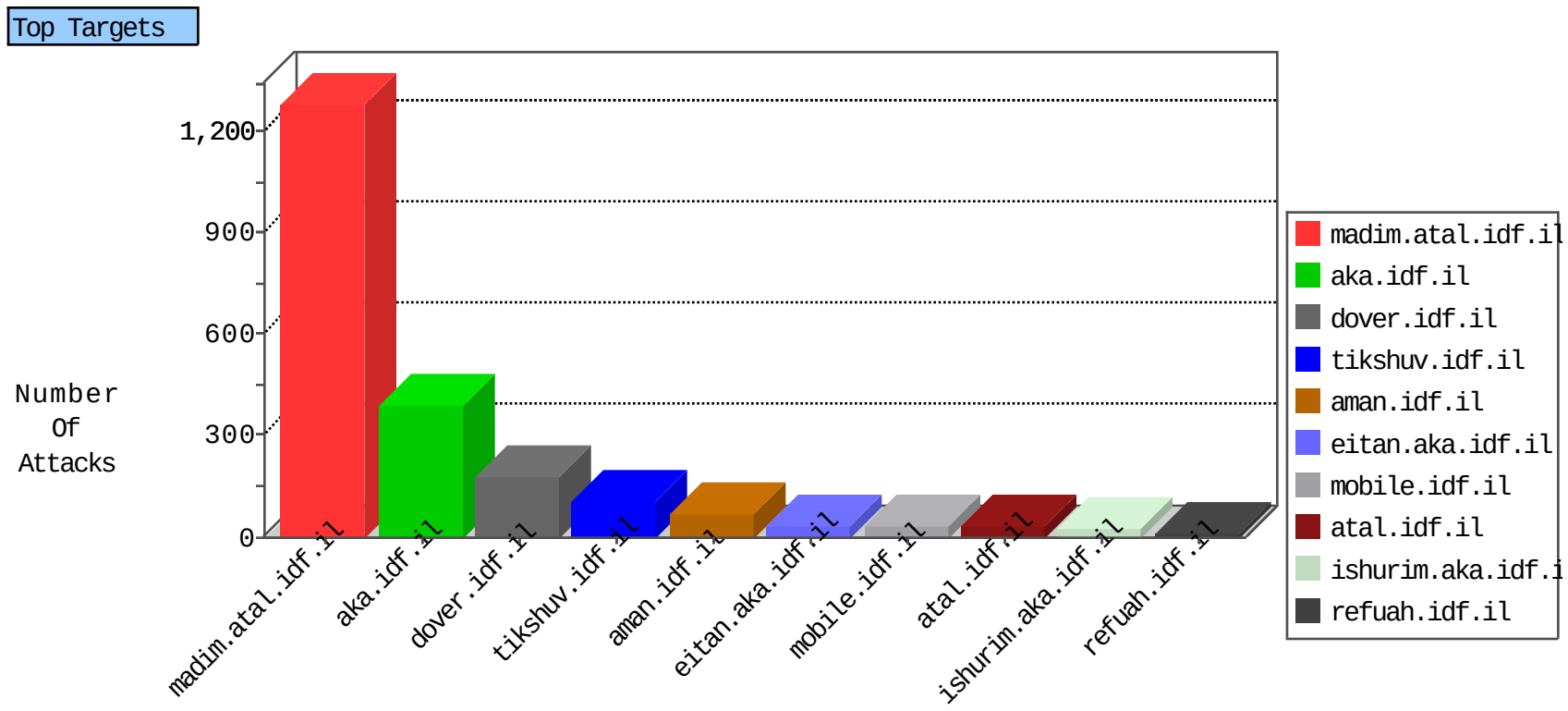
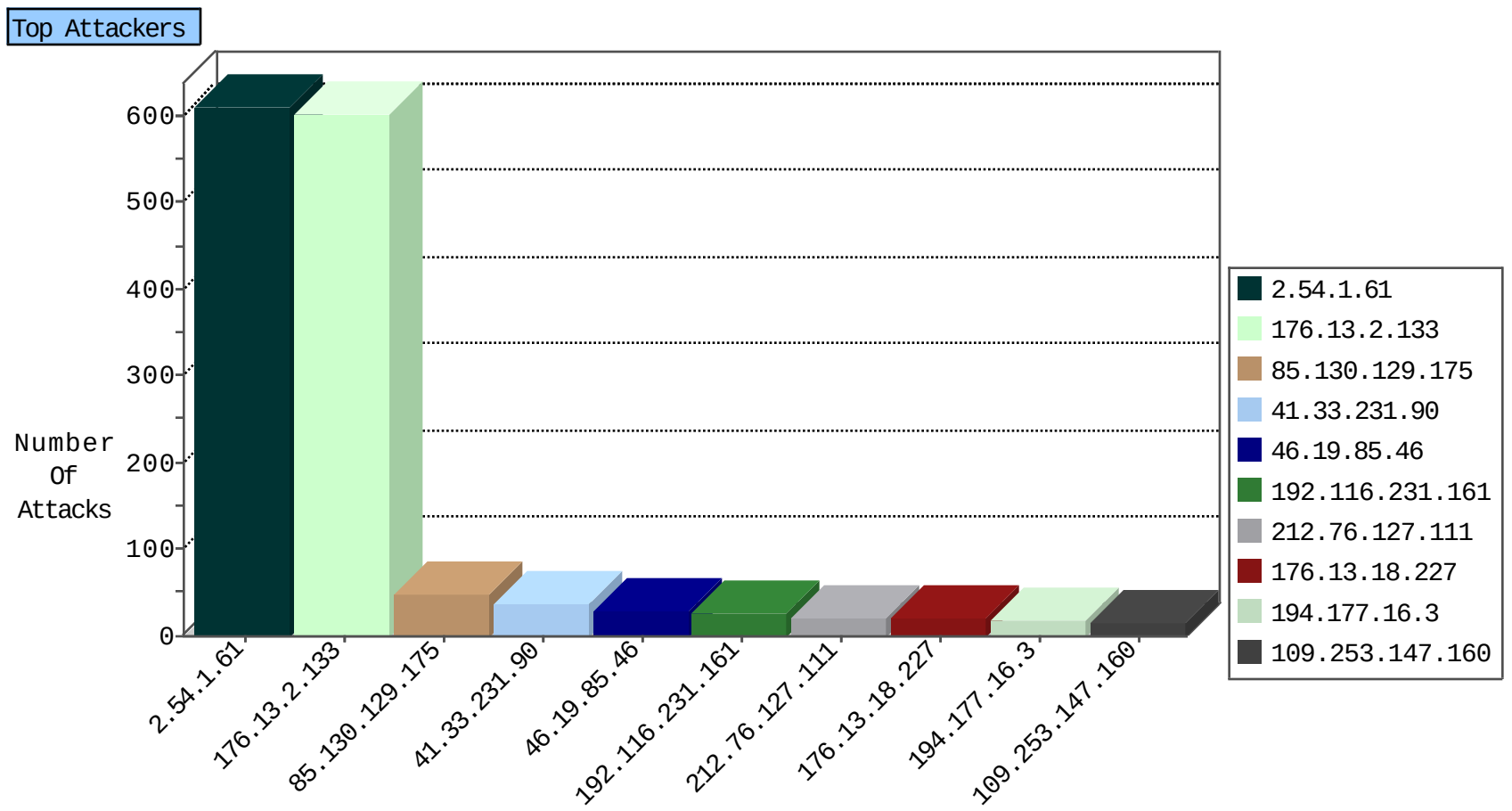
02-08-2016-17:04:03 to 02-08-2016-18:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-08-2016-17:04:03 to 02-08-2016-18:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
159.122.252.41	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
198.48.92.104	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
83.21.204.144	Poland	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
83.21.204.144	Poland	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

02-08-2016-17:04:03 to 02-08-2016-18:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.216.115.8		147.237.77.216	dover.idf.i	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	2

02-08-2016-17:04:03 to 02-08-2016-18:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.3.144.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.228.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.235.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.193.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.162.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.56	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.200.179	147.237.72.166	Israel	aka.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
171.80.212.153	147.237.76.86	China	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
84.228.176.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.166.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.175.126	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.253.96.122	147.237.77.205	China	prisha.idf.i	ET SCAN NMAP -sS window 3072	1
46.19.85.228	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.74.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.16.78.34	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1

02-08-2016-17:04:03 to 02-08-2016-18:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
192.116.231.161	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	21
176.13.18.227	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
194.177.16.3	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
109.186.148.199	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
185.32.179.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
212.117.136.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.28.137.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.234	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.49.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.26.147.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.14.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.178.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.76.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
166.170.28.41	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.204	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.81.48.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.133.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.135	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.52.14	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.155.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.255	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.145.217.24	Europe	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.53.0	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.133.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
84.108.168.225	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
212.25.107.145	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.155	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
81.218.44.19	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.108.168.225	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	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
46.19.86.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
130.203.136.75	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
5.22.134.194	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.169.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.190.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.123.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.1.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.169.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.57.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-08-2016-17:04:03 to 02-08-2016-18:04:03

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
5.22.134.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.1.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	354
176.13.2.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	315
176.13.2.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	270
2.54.1.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	184
2.54.1.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	69
85.130.129.175	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
46.19.85.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
176.13.2.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	17
85.250.186.202	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
109.253.147.160	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
82.145.217.24	Europe	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
2.54.1.61	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.54.1.61	Block	4
46.19.86.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
84.109.114.79	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	4
84.109.114.79	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/4/	Block	3
109.186.148.199	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
62.210.101.170	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.210.101.170	Block	3
176.13.0.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
178.71.170.229	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/givus	Block	2
84.111.110.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$74 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
2.54.169.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.182.125.234	Israel	147.237.76.42	refuah.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.52.173.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.215.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.136.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.7.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.224	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.66.52.78	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.54.133.201	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.127.63.81	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
149.88.147.137	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.88.147.137	Block	1
62.210.101.170	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/feed	Block	1
188.143.232.10	Russian Federation	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker	Block	1
66.249.65.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.117.199.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
178.71.170.229	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/givus	Block	1
149.88.147.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/matash	Block	1
62.219.120.114	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
2.54.1.61	Israel	147.237.0.19	madim.atal.idf.i	Too Many 403: Response Code per Session	Block	1
213.151.42.84	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
84.109.112.150	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$20 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.120.159.0	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.111.110.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
5.28.156.172	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/def	Block	1
79.182.171.108	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
185.25.151.159	Poland	147.237.72.156	aman.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
157.55.39.100	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/military-police/	Block	1