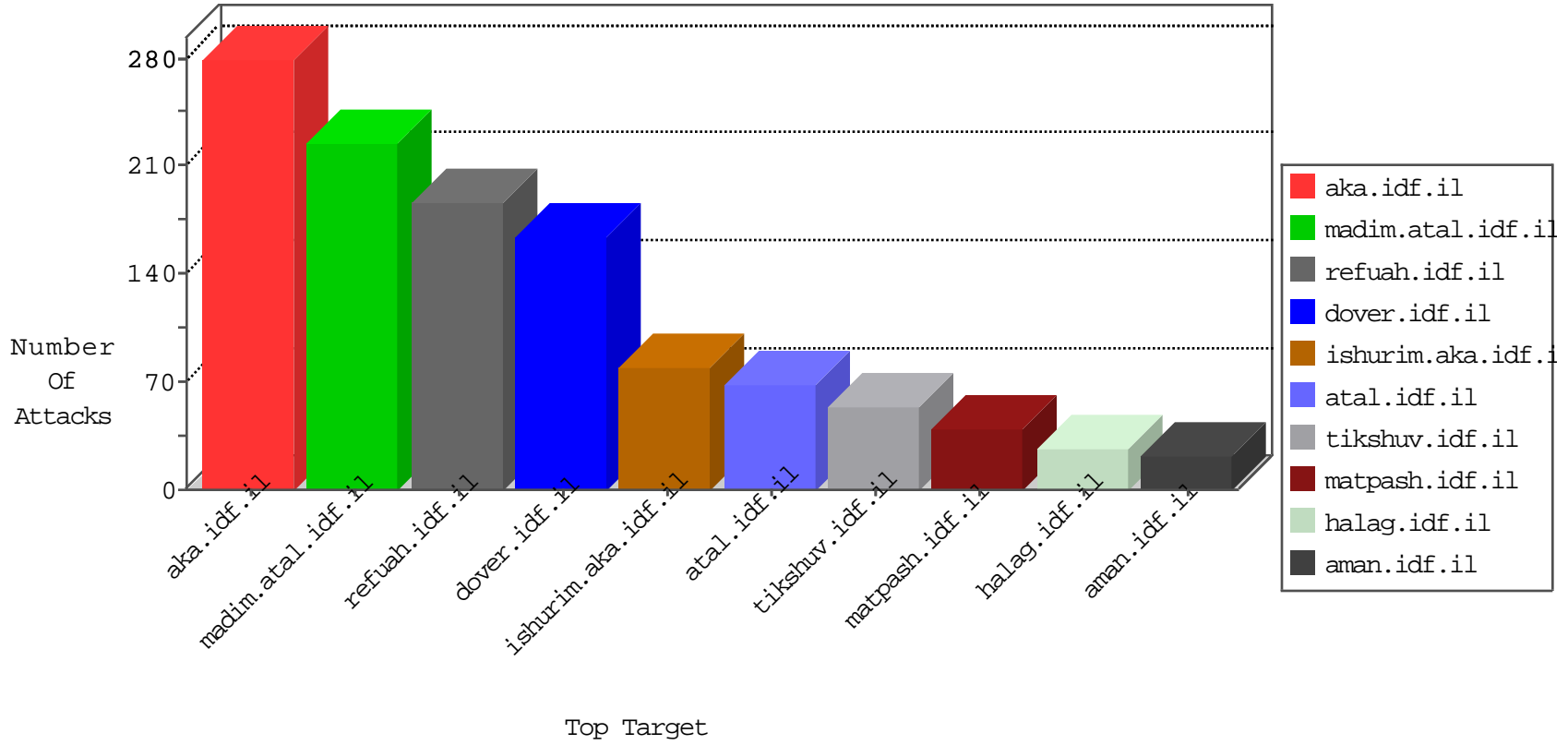


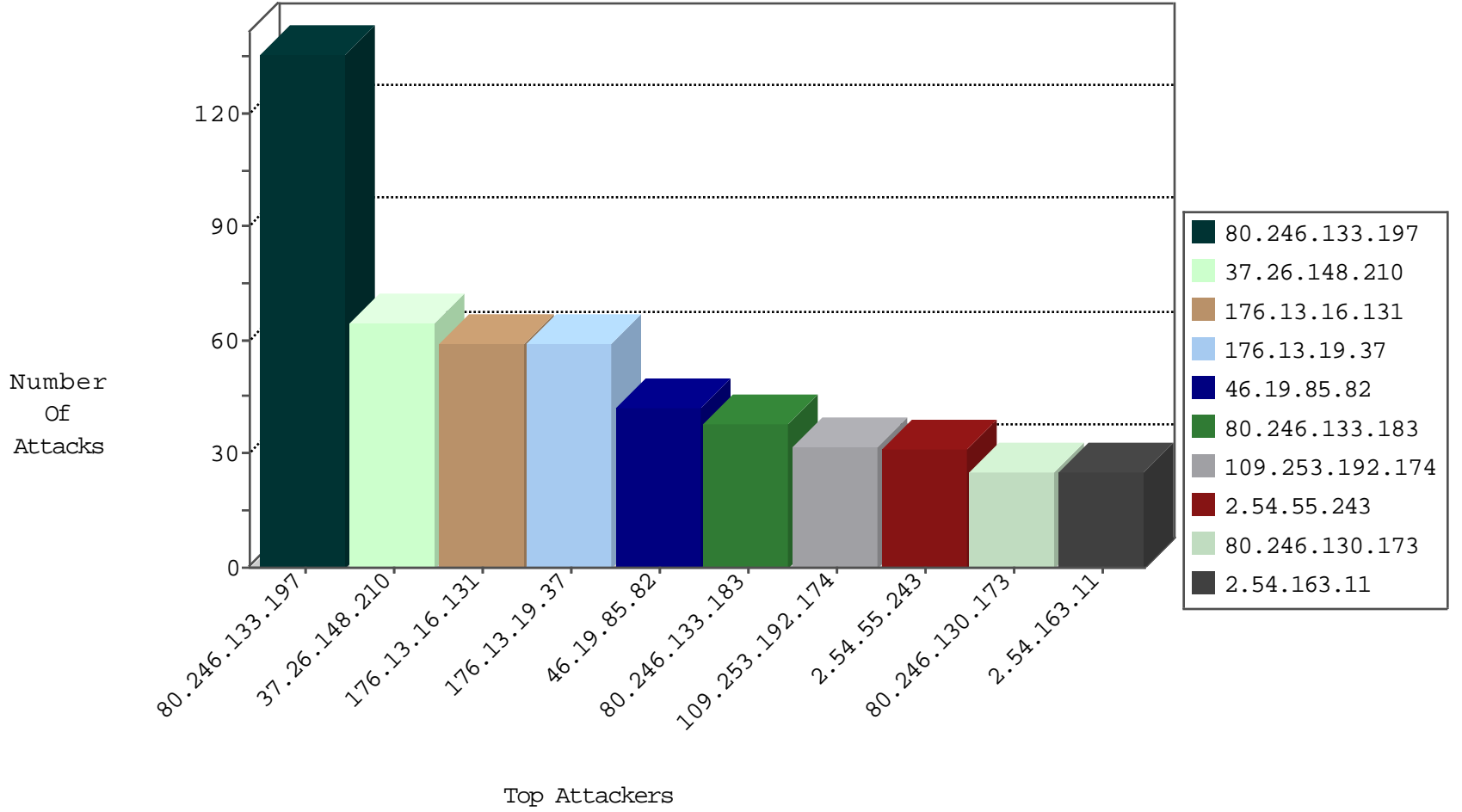
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.118.30.102	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	150
82.145.216.77	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	22
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	4
79.182.23.89	Israel	147.237.0.34	tikshuv.idf.il	L4 Source or Dest Port Zero	drop	3
134.147.203.115	Germany	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
58.97.111.9	Thailand	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1
58.97.111.10	Thailand	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.223	France	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1
180.251.137.58	Indonesia	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
180.251.137.58	147.237.77.216	Indonesia	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	3
79.176.161.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.99.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.170.70.222	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.54.4.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.120.126.35	147.237.72.166		aka.idf.il	portscan: TCP Distributed Portscan	1
109.226.48.114	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.95.226.189	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
75.147.243.2	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.216.174	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.132.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.162.124	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
149.78.79.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.193.51.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.133.197	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	134
46.19.85.82	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	39
66.249.81.175	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	24
80.246.130.173	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
66.249.81.183	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	23
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
66.249.81.179	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	18
82.102.228.90	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	17
37.26.148.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
37.26.148.210	Israel	147.237.72.166	aka.idf.il	drop		drop	15
37.26.148.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
37.26.148.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.32.121.153	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
89.139.166.186	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
77.127.198.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
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
80.178.134.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
80.246.133.211	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
192.198.151.44	Europe	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.0.244.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.66.96.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.131.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.116.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.222.1	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
37.26.148.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.8.11	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.9.3	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
62.0.222.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.147.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
95.86.112.2	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.93.250	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
82.80.132.76	Israel	147.237.77.216	dover.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
2.54.55.243	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.21.235	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.93.56	Israel	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
149.78.211.185	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
1.20.211.160	Thailand	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
37.26.146.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
176.13.23.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.176.188.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.82	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.46.212	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.16.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
176.13.19.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
80.246.133.183	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.133.183	Block	37
109.253.192.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
2.54.55.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
2.54.163.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
91.193.51.97	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
109.253.147.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.99	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	5
109.253.144.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.137.101	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	3
109.253.208.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.143.172.178	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.143.172.178	Block	2
82.205.113.88	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ping	Block	2
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	2
79.176.120.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.48.204	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
37.187.114.171	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to /sap/hana/admin/	Block	1
207.46.13.127	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
2.54.44.65	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.99.32.51		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1086-17966-en	Block	1
89.138.163.21	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
176.13.14.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct107.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
62.90.9.250	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct165 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
5.29.163.108	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/titlecap.png	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.23.9	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in URL	Block	1
79.177.58.171	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
212.199.76.35	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 212.199.76.35 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
185.120.126.5		147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
89.139.166.186	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.14.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct150.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
80.246.133.197	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
95.143.172.178	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
31.13.99.103	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
192.117.129.166	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.166.148.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.205.65.186	United Arab Emirates	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
79.181.116.208	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/main/home/default.aspx	Block	1
46.19.85.215	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$78 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
212.199.76.35	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 192.115.64.250	Block	1
80.246.133.211	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/scriptresource.axd	Block	1