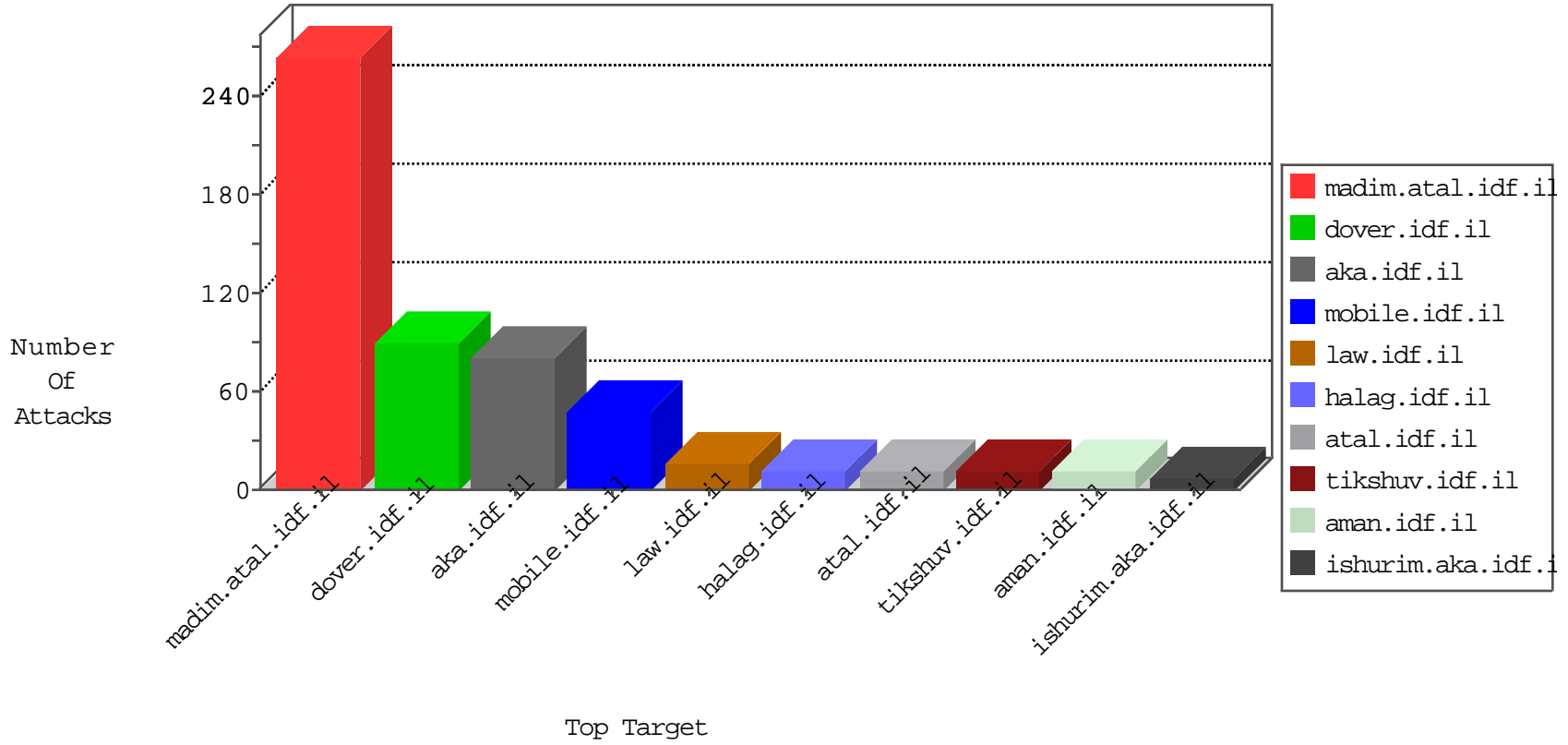


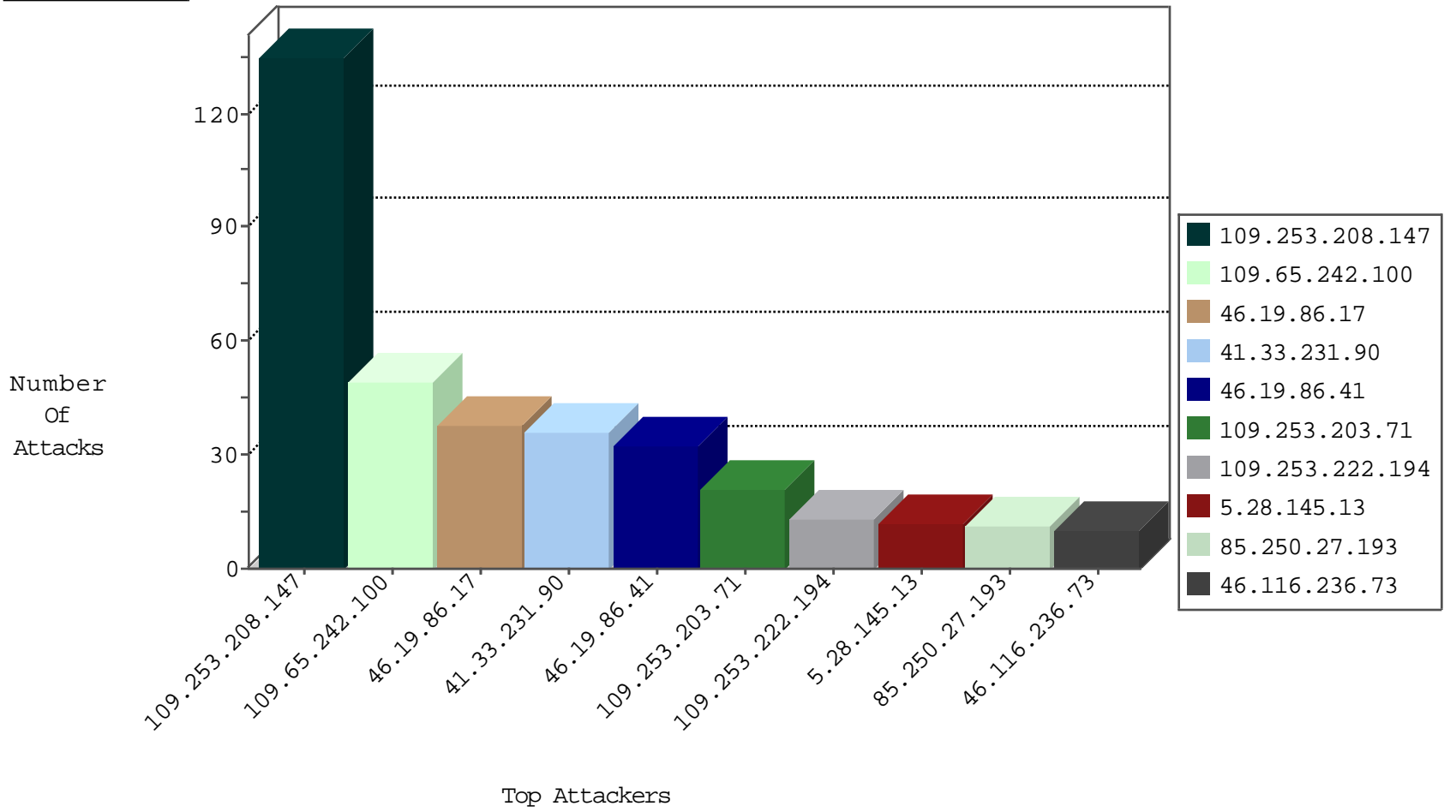
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	2
115.239.228.10	China	147.237.0.34	tikshuv.idf.il	JLM_Under_Attack_Con_Http	drop	2
184.105.139.106	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
205.209.185.11	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.113	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
216.218.206.121	United States	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.73	United States	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.118	United States	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
115.239.228.10	China	147.237.0.34	tikshuv.idf.il	JLM_Purple_Con_Limit_Http	drop	1
184.105.139.82	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.118	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.22.47.242	Finland	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
51.255.65.50	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	2
85.64.2.84	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.255.65.46	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.18	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.70	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.28	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.88	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.37	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	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
178.18.17.201	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
123.8.183.110	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
208.80.155.214	147.237.77.176	United States	matpash.idf.il	Tehila - Perl LWP with fake user agent	1
180.97.81.71	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
178.18.17.201	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1

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
46.19.86.17	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
5.28.145.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
5.102.207.225	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.179.172	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.116.236.73	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.116.236.73	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
79.177.154.149	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.128	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.39.169	Israel	147.237.77.216	dover.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
85.250.27.193	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
149.78.3.165	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
85.250.27.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.65.201.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.54.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.3.165	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.54	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.134.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.151.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.76.147	chimuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.173.46.108	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
213.8.204.24	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
185.3.147.117	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
31.210.179.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.197.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.164.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.41.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.22.10	Israel	147.237.76.86	navy.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
213.57.162.208	Israel	147.237.0.34	tikshuv.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
40.77.167.63	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
85.250.27.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.8.204.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
157.55.39.249	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
213.8.204.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
85.65.47.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
188.29.165.9	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.54.134.229	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.10	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.228.169.44	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.117.207.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.108	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.80.155.214	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
79.180.120.134	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.235	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.208.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	135
109.65.242.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
46.19.86.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
109.253.203.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
109.253.222.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
46.19.86.17	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.138.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.138.75.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.78.105.47	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
79.180.20.127	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
157.55.39.245	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-23092-h/dover.aspx	Block	1
74.82.47.4	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
219.94.128.197	Japan	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
37.218.214.215	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
149.78.51.36	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1
93.173.46.108	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
46.19.86.17	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
2.52.63.210	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
178.92.46.134	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
77.125.152.234	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
95.221.251.64	Russian Federation	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
178.92.46.134	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
131.253.25.216	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.61	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
149.78.252.3	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ctl100\$cphMain\$cphSachar\$ctl137 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.79.202	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list6.htm	Block	1
5.102.207.225	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.3.146.67	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ctl100\$cphMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
149.78.8.48	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 149.78.8.48 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
157.55.39.154	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
31.210.179.172	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
213.8.204.79	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/giyus	Block	1
149.78.8.48	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
91.250.33.201	Ukraine	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1