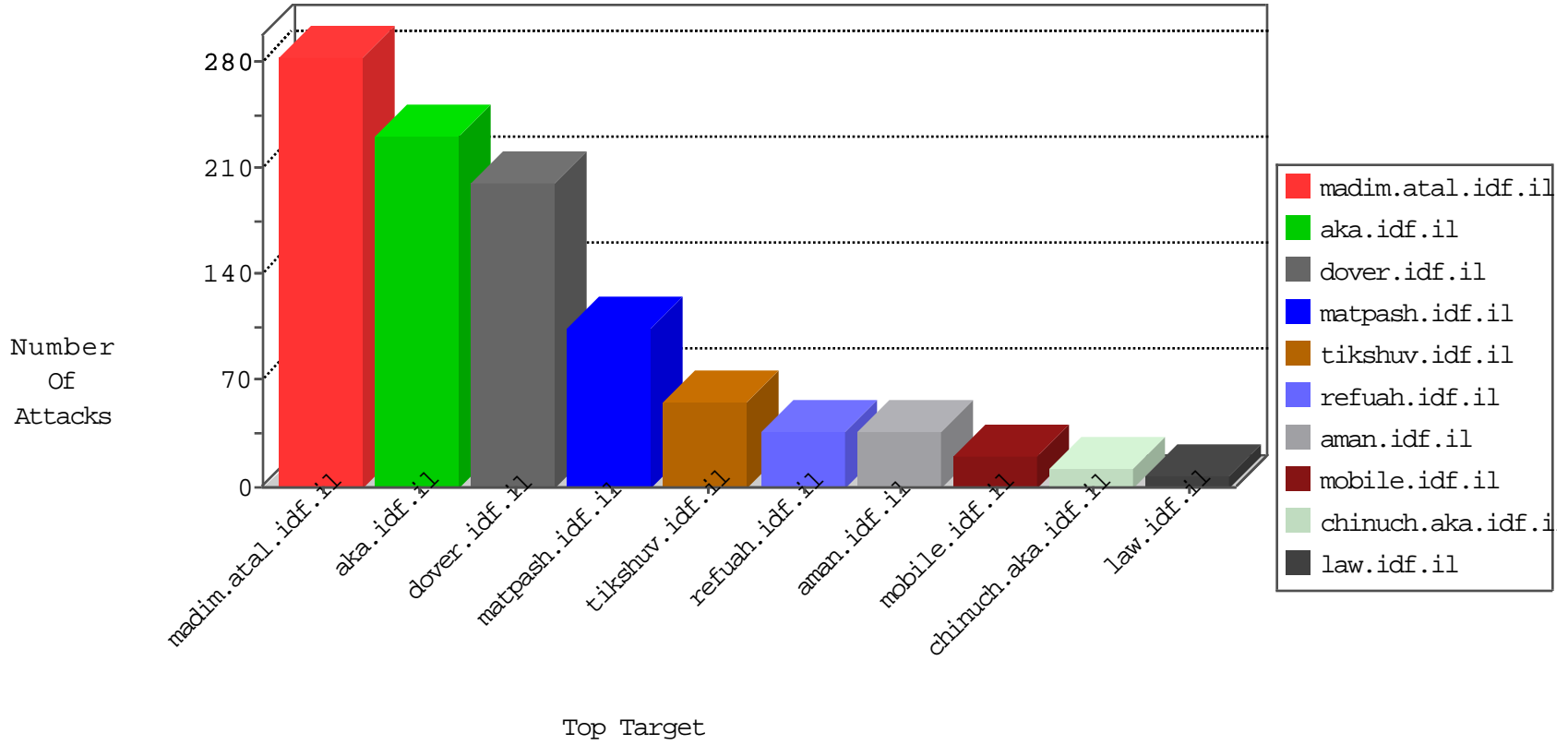


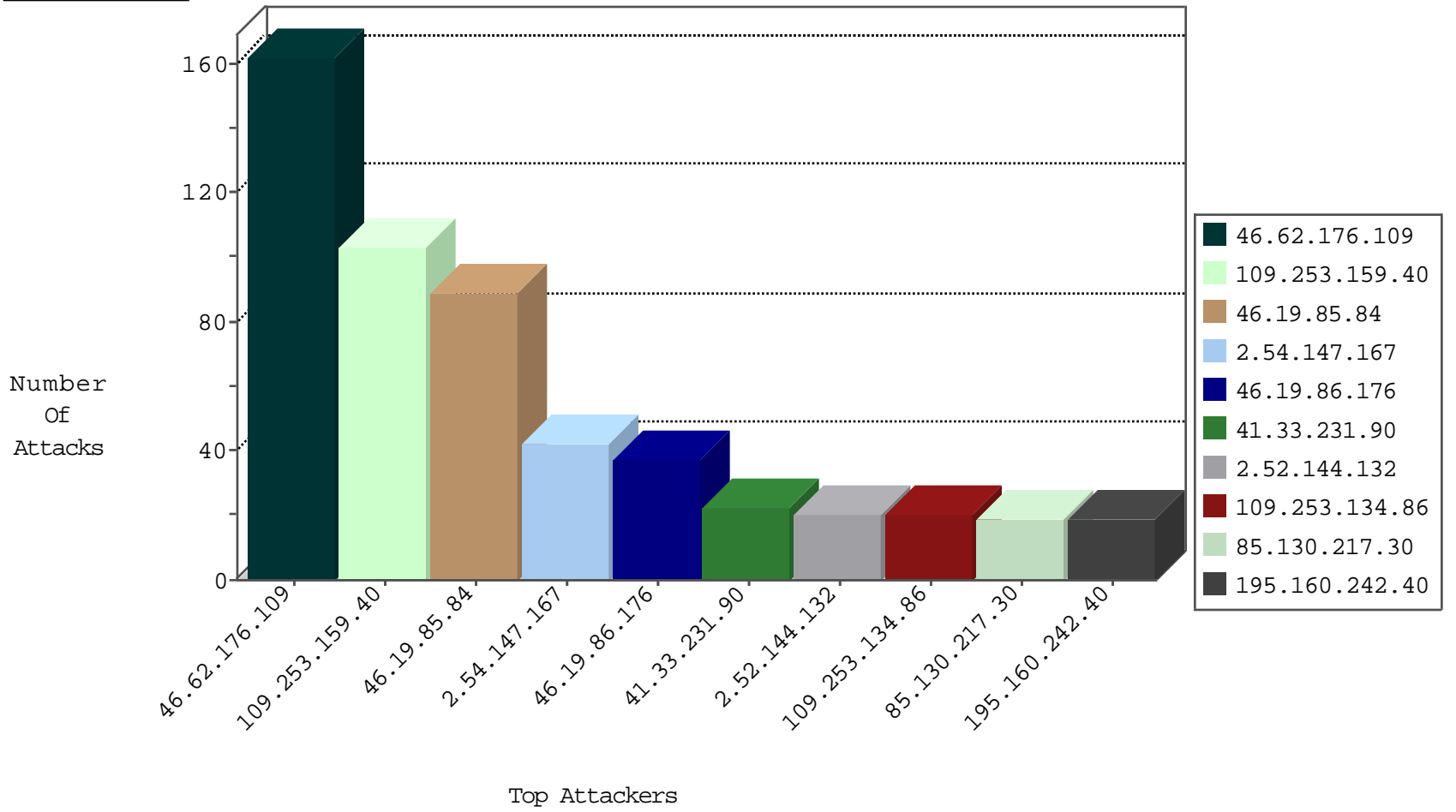
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
107.150.33.62	United States	147.237.77.176	matpash.idf.il	block-sp-trafl	drop	1
115.239.228.10	China	147.237.76.201	e.atal.idf.il	JIM_Purple_Con_Limit_Http	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.102.214.151	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
192.116.55.245	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
61.160.195.5	China	147.237.77.176	matpash.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.19.108	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
2.54.157.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
122.236.118.186	147.237.77.170	China	maarachot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.193	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
89.138.178.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.176.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.34.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
212.235.98.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
2.54.179.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
2.54.36.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.214.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
84.228.41.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.76	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
69.64.46.86	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
213.57.253.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.62.176.109	Iran, Islamic Republic of	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	51
2.54.147.167	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
46.62.176.109	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	41
46.62.176.109	Iran, Islamic Republic of	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	37
46.62.176.109	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
195.160.242.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
85.130.217.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.52.144.132	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.54.147.158	Israel	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
195.160.242.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
188.120.148.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.48.213	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
85.130.132.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
5.22.129.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.132.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.52.144.132	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
2.52.169.215	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
141.0.13.48	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.144.132	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.87.224.100	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.253.23.154	Switzerland	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
201.173.39.143	Mexico	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
199.30.24.75	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.130.217.30	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.199	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
217.132.9.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.200.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.153.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.134.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.45.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.217.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
31.168.220.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.130	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.179.13.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	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
217.132.67.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.18.35	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.253.211.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.92.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.141.29	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
194.90.216.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.14.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.116.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.35.132.190	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.159.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	103
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
46.19.86.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
109.253.134.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
46.19.86.244	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	18
46.19.85.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
168.63.139.43	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
80.246.130.248	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
222.172.46.224	China	147.237.76.147	chinuch.aka.idf.il	PHP Attempt	Block	5
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
222.172.46.224	China	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 222.172.46.224	Block	4
66.249.81.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.86.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.109.116.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.138.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.116.149.197	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/894-he/refuah.aspx -	Block	3
176.13.13.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.15.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	2
176.13.22.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.130.247	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.109	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	2
46.119.117.85	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	2
80.178.186.11	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.253.23.154	Switzerland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
31.154.41.13	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
222.172.46.224	China	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/plus/download.php	Block	1
80.246.130.106	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
149.88.58.169	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
62.219.254.97	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	1
46.19.85.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
104.131.214.84	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 104.131.214.84	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.52.144.35	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
212.199.142.58	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
80.178.186.12	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.116.183.143	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
85.64.243.0	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1242-he/atal.aspx	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
104.131.214.84	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/14-he	Block	1
83.130.127.24	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
2.54.51.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
216.72.40.185	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
80.178.187.228	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.116.95.240	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
128.232.110.28	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1