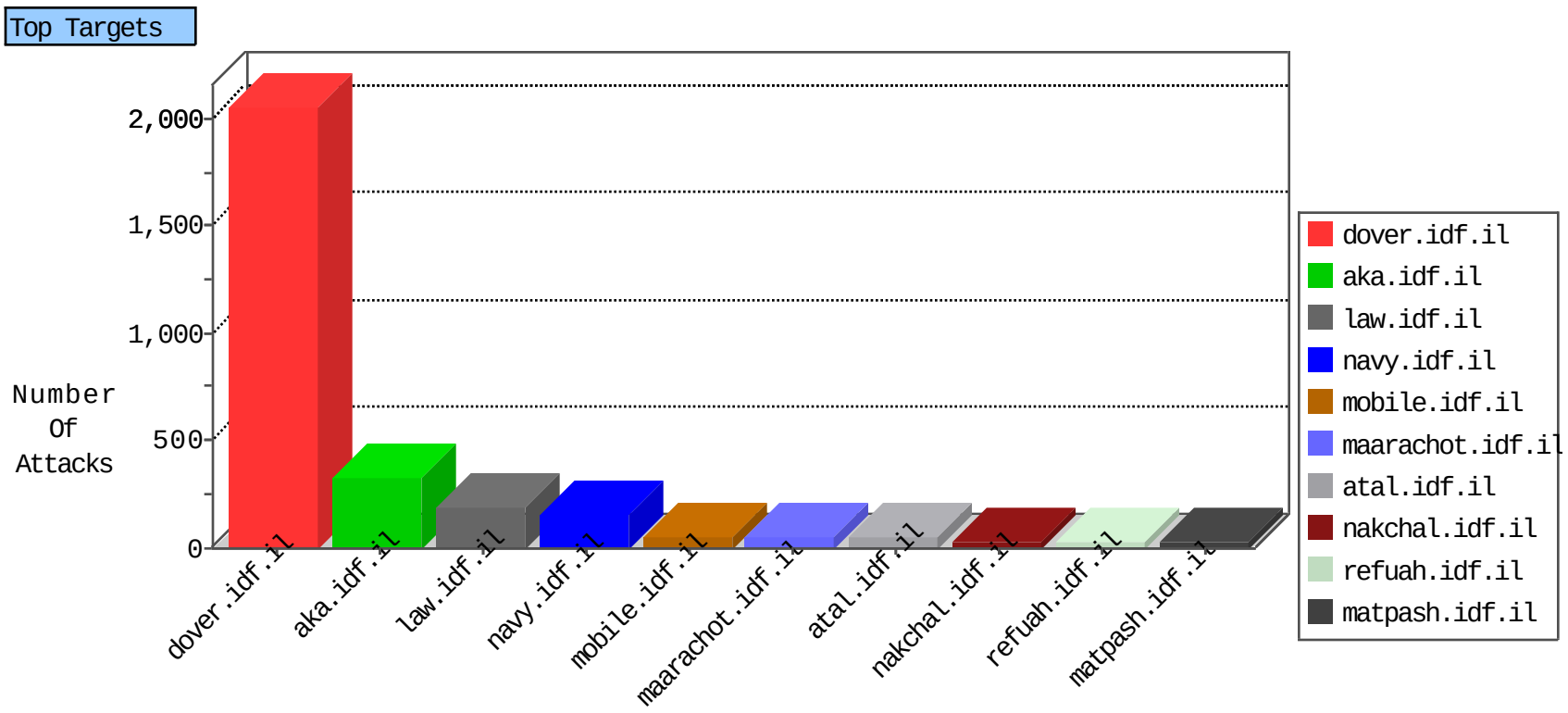
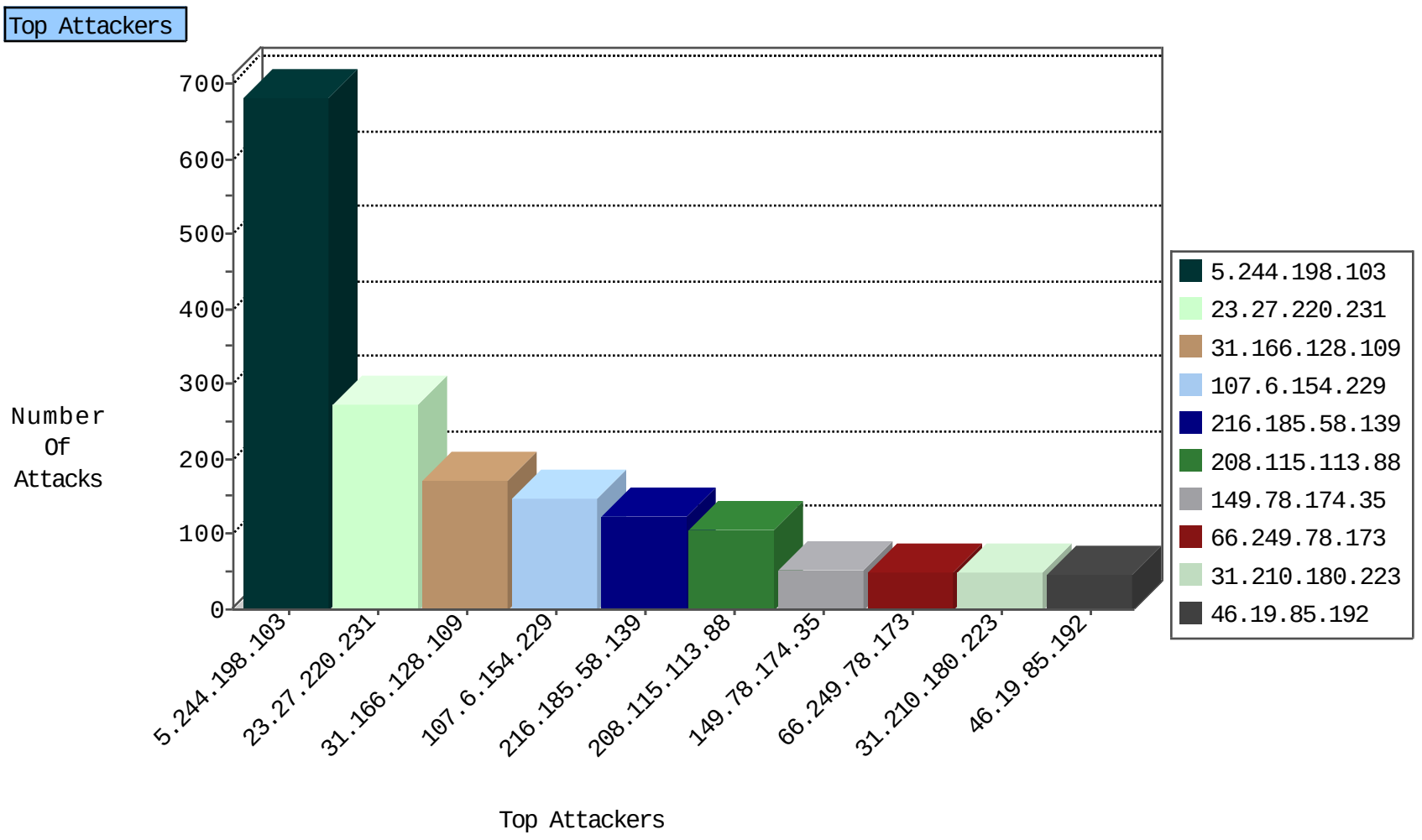
10-31-2015-08:04:07 to 10-31-2015-09:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-31-2015-08:04:07 to 10-31-2015-09:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	8739
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1670
107.6.154.229	Netherlands	147.237.77.74	law.idf.il	TCP Scan (vertical)	drop	1323
66.249.75.68	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	758
79.182.137.42	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	91
84.228.110.76	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	64
72.9.148.10	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	44
85.65.101.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
176.13.15.72	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
5.9.88.82	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
85.65.16.128	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
46.117.76.222	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
31.154.254.78	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
107.6.154.229	Netherlands	147.237.77.74	law.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
94.210.158.144	Netherlands	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
66.249.67.65	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
149.78.104.57	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
5.244.198.103	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.69.84	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.186.90	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
66.249.75.60	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.85.146	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
204.42.253.132	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-31-2015-08:04:07 to 10-31-2015-09:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
107.6.154.229	Netherlands	147.237.77.74	law.idf.il	10767: HTTP: Acunetix Security Scanner	Block	1
198.20.69.74	United States	147.237.8.46	e.chinuch.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

10-31-2015-08:04:07 to 10-31-2015-09:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

10-31-2015-08:04:07 to 10-31-2015-09:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.244.198.103	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	441
23.27.220.231	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	272
5.244.198.103	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	194
31.166.128.109	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	172
216.185.58.139	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	123
31.210.180.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
5.244.198.103	Saudi Arabia	147.237.77.216	dover.idf.il	drop		drop	35
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
176.13.15.72	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.85.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
84.228.110.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
100.100.121.178		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
106.77.17.114	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
5.244.198.103	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.179.28.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.34	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
176.106.46.79	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.0	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
77.127.238.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.65.101.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
100.100.56.200		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
213.57.136.91	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
100.100.80.223		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.136	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
194.150.168.95	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.117.76.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
94.210.158.144	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.9.88.82	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
162.243.192.180	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
213.57.143.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	90
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	30
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	30
149.78.174.35	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	30
66.249.69.81	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1492-he/atal.aspx	Block	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	15
5.29.126.239	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	15
107.6.154.229	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he/	Block	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	15
157.55.39.86	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	15
46.117.100.25	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	15
82.213.13.62	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4466.jpg	Block	15
66.249.69.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	15
141.212.121.192	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/	Block	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/fence-	Block	15
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/105962.pdf	Block	15
46.120.240.101	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	15
83.71.247.34	Ireland	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	15
66.249.75.54	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/5/225.pdf	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
46.19.85.192	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	15
149.78.174.35	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	15
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/yoman.asp	Block	15
66.249.65.139	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/articles.aspx	Block	15
5.29.62.234	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	15
84.108.250.47	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/april/1.	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.122	Block	15
46.19.85.192	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	15
79.177.41.37	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	15
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	15
5.29.126.114	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	15
85.93.91.84	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1158-he/dover.aspx	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1148-he/chinuch.aspx	Block	15
149.88.82.120	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	15
46.19.85.192	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	15
82.118.237.111	Bulgaria	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	15