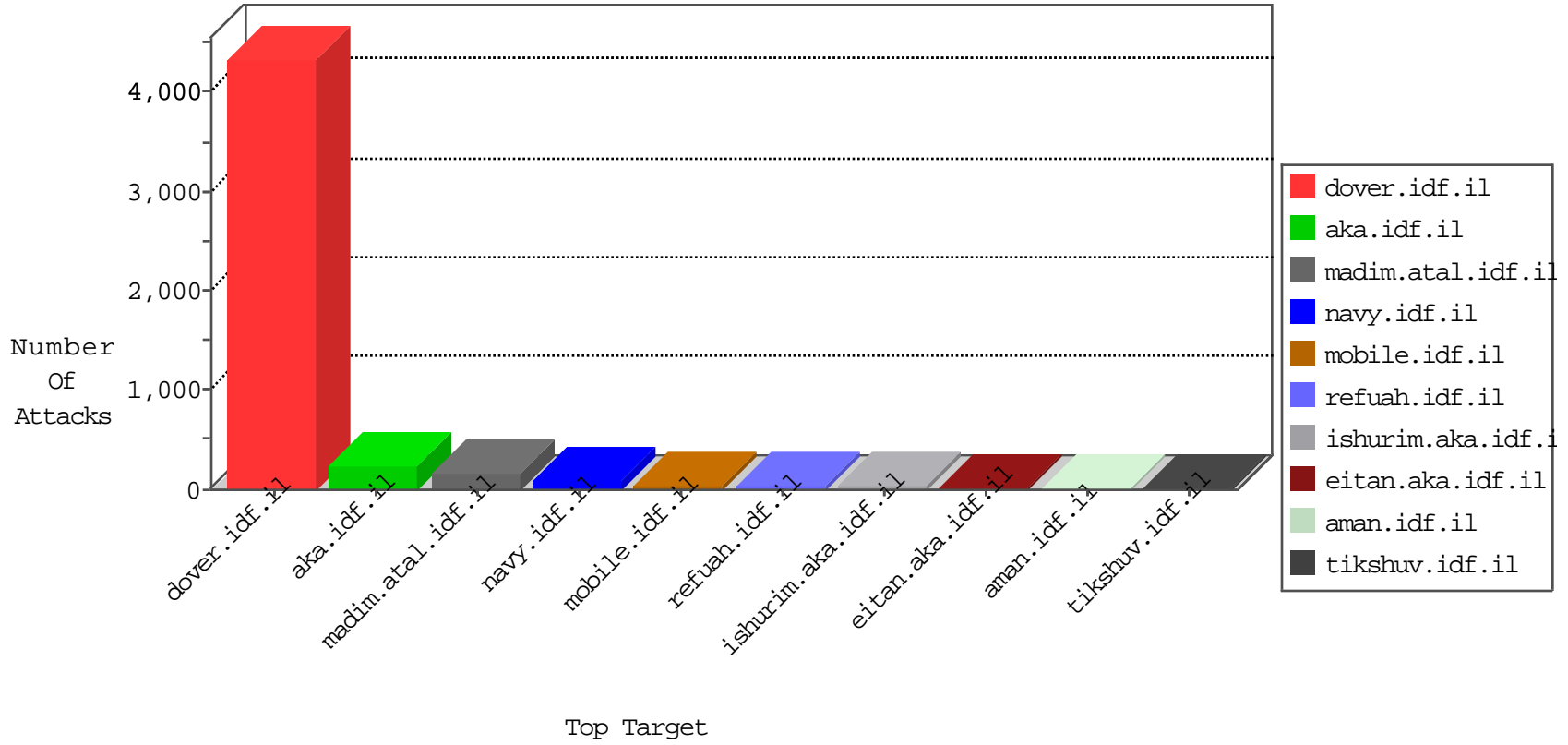


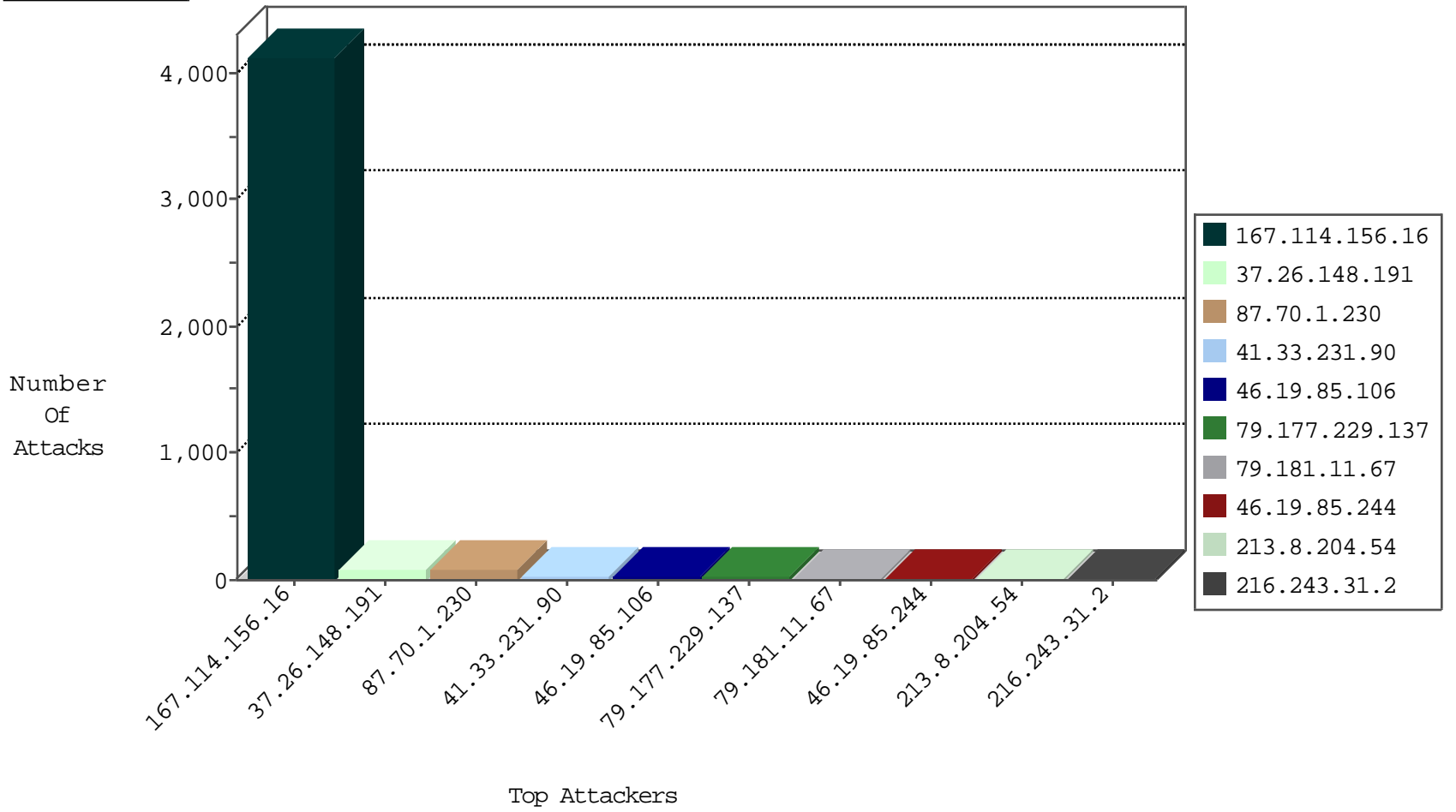
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4117
79.178.205.207	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
124.107.243.130	Philippines	147.237.0.200	m4u.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
82.145.220.9	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	2
134.147.203.115	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	2
101.201.147.32	China	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	2
209.126.110.228	United States	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1
209.126.110.228	United States	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
185.70.184.187	Netherlands	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
109.67.176.219	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
89.139.247.1	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
176.9.10.227	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	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	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
2.53.166.11	Israel	147.237.72.167	ishurim.aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	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
61.149.161.186	147.237.72.166	China	aka.idf.il	GPL SCAN nmap TCP	2
37.26.148.191	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
59.103.76.109	147.237.77.170	Pakistan	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
59.103.76.109	147.237.77.170	Pakistan	maarachot.idf.il	ET SCAN NMAP -f -sS	1
46.4.79.76	147.237.76.86	Germany	navy.idf.il	ET SCAN NMAP -sS window 1024	1
118.193.20.114	147.237.76.176	Hong Kong	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
85.64.104.255	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.103.76.109	147.237.77.170	Pakistan	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
46.4.79.76	147.237.77.19	Germany	law-forum.idf.il	ET SCAN Potential SSH Scan	1
193.219.125.17	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
115.29.197.215	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.76.30	Netherlands	himush.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	30
79.181.11.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
213.8.204.54	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
46.19.85.244	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
79.179.220.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.14.135	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
80.246.136.43	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
11.15.119.240	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.23.109	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
78.175.164.45	Turkey	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
185.32.179.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.188.123	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.195.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.38.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.139.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.56.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.65.37.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.106	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.106.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.107	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.229.137	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.106	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
63.141.204.105	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.71.34.28	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.229.137	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
176.13.23.109	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
188.120.148.108	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.166.11	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.64.36.131	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.220	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.29.8.147	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.86	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.177.229.137	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
199.30.24.188	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.177.229.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
85.64.36.131	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.53.129.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.138.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.220	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
31.210.188.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.3.144.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.53.26.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.145.232	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
87.70.1.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
46.120.212.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
157.55.39.210	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.210	Block	3
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
79.183.39.36	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 79.183.39.36	Block	3
46.116.221.166	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
149.78.38.76	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	2
79.183.39.36	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/mobile	Block	2
46.19.86.134	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
185.32.179.214	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.22.130.75	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
109.64.62.98	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
79.180.135.91	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct113 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2726.jpg	Block	1
82.102.136.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
199.30.24.10	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.64.141.101	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
31.154.50.181	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
79.183.39.36	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/templates/newslobby/mobile	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/sitemap/sitemap.aspx	Block	1
173.252.90.105	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
37.142.240.15	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/newslobby/mobile	Block	1
84.108.168.159	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
66.249.79.108	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1407-he/atal.aspx	Block	1
199.203.64.23	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 199.203.64.23	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	1
31.210.188.123	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
37.142.253.217	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
176.13.14.135	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout2.css	Block	1
50.7.82.66	Spain	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
199.203.64.23	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/templates/homepage/mobile	Block	1
31.210.188.123	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
40.77.167.25	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17899-he/dover.aspx   f :• ½ , é , -f ½ , é , -f ½ , é , -	Block	1
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
2.55.26.168	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/favicon.ico	Block	1
95.86.93.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
77.124.22.200	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/newslobby/mobile	Block	1
207.46.13.178	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/wut	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.163	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/miluum/default.aspx	Block	1
37.26.147.213	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
82.81.102.108	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2347.jpg	Block	1