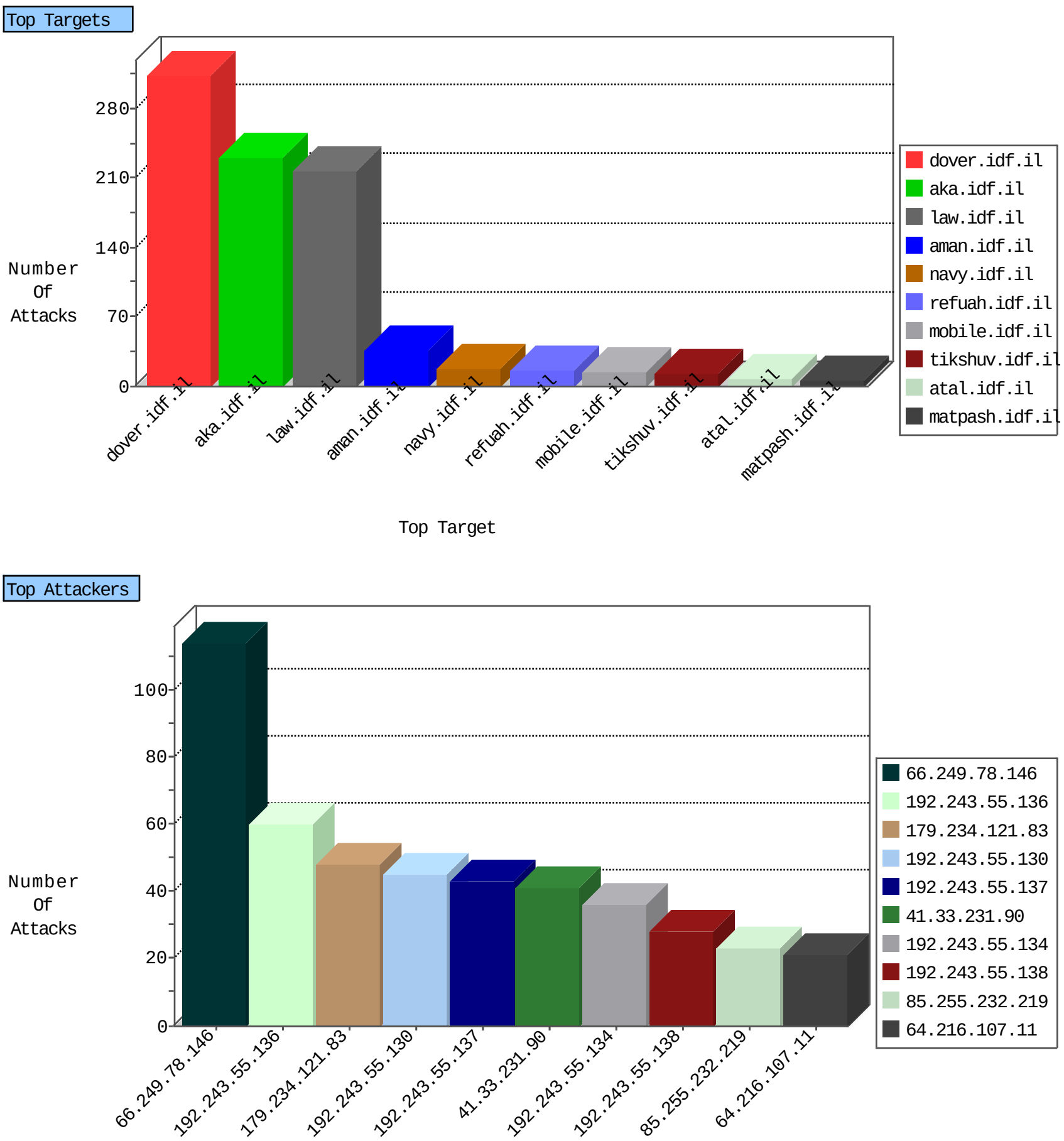
04-23-2016-18:04:06 to 04-23-2016-19:04:06

IDF Under Attack Daily Report



04-23-2016-18:04:06 to 04-23-2016-19:04:06

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	TCP handshake violation, first packet not syn	drop	11542
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	4
185.94.111.1	Russian Federation	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.99	Lithuania	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1
104.238.135.152	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

04-23-2016-18:04:06 to 04-23-2016-19:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-23-2016-18:04:06 to 04-23-2016-19:04:06

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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.66.17	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
2.53.191.220	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
76.181.249.213	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
76.181.249.213	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
220.134.34.86	147.237.0.34	Taiwan	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.248.100.195	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
115.182.17.13	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
104.219.238.10	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 4096	1
94.255.224.2	147.237.77.226	Sweden	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
76.181.249.213	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.54.169	147.237.76.42	France	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
189.219.139.119	147.237.0.16	Mexico	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
115.182.17.13	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
104.219.238.10	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
98.126.212.154	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1

04-23-2016-18:04:06 to 04-23-2016-19:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	114
179.234.121.83	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	27
85.255.232.219	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
64.216.107.11	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
207.241.231.194	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	19
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
176.13.8.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
120.146.153.24	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
99.59.108.161	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
212.40.139.38	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
192.243.55.130	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.136	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.130	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.128.48.46	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
66.249.66.184	United States	147.237.0.34	tikshuv.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.109.197	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.128.48.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.70.109.197	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.134	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
40.77.167.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.138	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.137	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
2.53.4.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	4
157.55.39.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

04-23-2016-18:04:06 to 04-23-2016-19:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.197.155	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	4
2.53.191.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.180.200.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.197.155	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.253.197.155	Block	2
66.249.78.160	Israel	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/ishurim/cityofficers/	None	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/portalmiluim/templates/www.behazdaa.org.il	Block	1
2.55.142.195	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/994-8587-he/himush.aspx'	Block	1
74.91.20.195	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
184.168.200.134	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il/wordpress/wp-admin/	Block	1
84.228.253.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
38.111.147.84	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
217.115.112.107	Ireland	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il/test/wp-admin/	Block	1
119.81.50.222	Singapore	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il/blog/wp-admin/	Block	1
77.237.138.202	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
66.249.64.75	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/news/{"key":"	Block	1
184.168.200.228	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
41.200.247.222	Algeria	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
120.146.153.24	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1540-13036-he/dover.aspx target=	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
98.143.112.201	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il/old/wp-admin/	Block	1
74.91.18.44	United States	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on www.yun.ph/	Block	1
41.200.247.222	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
157.55.39.142	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
84.94.114.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
191.252.46.105	Brazil	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
74.91.18.44	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
46.19.86.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.21.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
84.228.253.216	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.228.253.216	Block	1

04-23-2016-18:04:06 to 04-23-2016-19:04:06