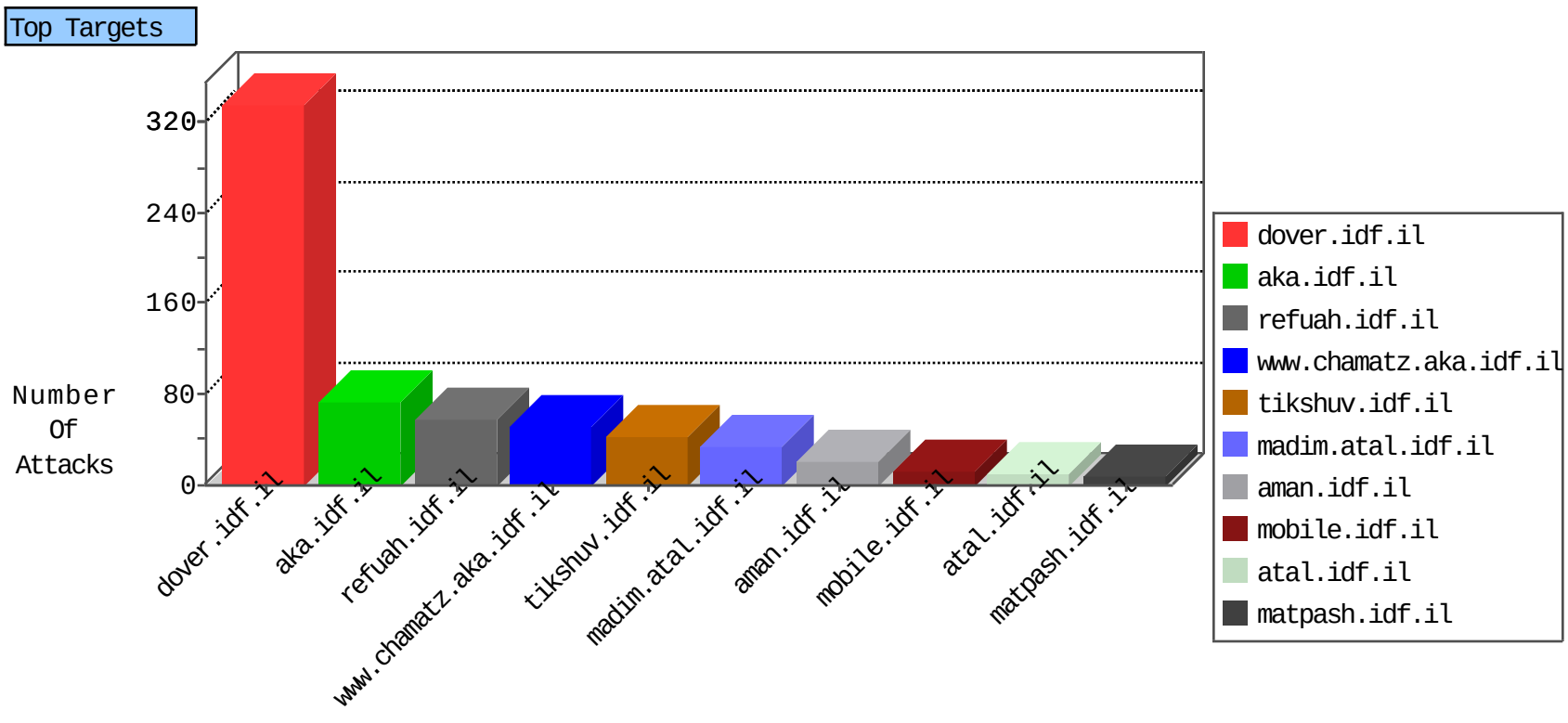
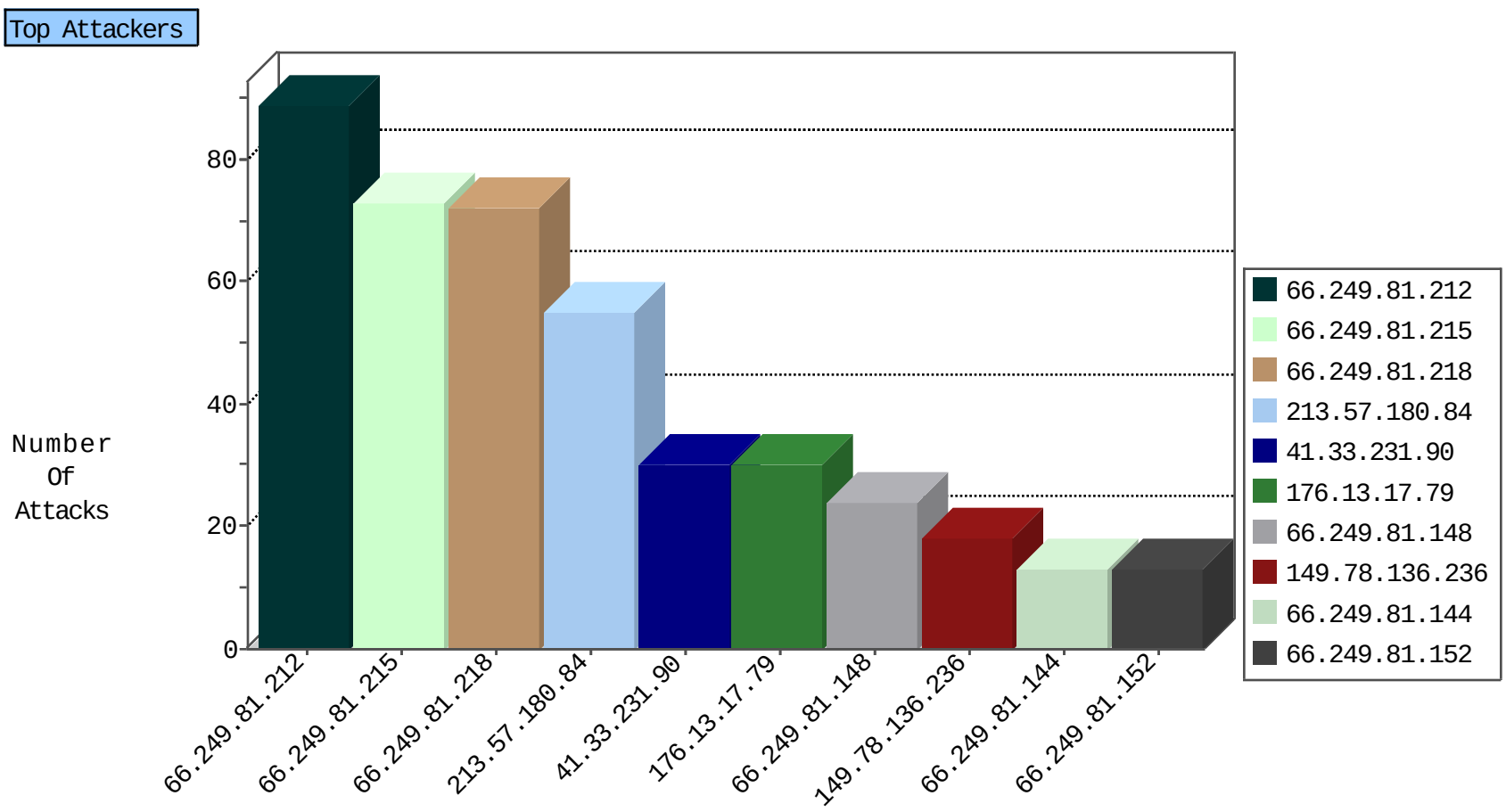
02-26-2016-21:04:04 to 02-26-2016-22:04:04

IDF Under Attack Daily Report





02-26-2016-21:04:04 to 02-26-2016-22:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.152.18	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	5
222.188.100.102	China	147.237.0.33	idf.il	Invalid TCP Flags	drop	2
179.43.141.219	Switzerland	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
217.26.171.188	Moldova, Republic of	147.237.77.176	matpash.idf.il	L4 Source or Dest Port Zero	drop	1
82.79.205.124	Romania	147.237.72.156	aman.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
179.43.141.219	Switzerland	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
185.106.92.87		147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
121.224.239.202	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
201.210.155.173	Venezuela	147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	1
39.161.46.235	China	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1

02-26-2016-21:04:04 to 02-26-2016-22:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.136.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
123.126.113.102	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
46.120.2.93	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
176.13.23.38	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
88.217.35.95	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	3
51.255.65.82	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.249.79.171	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1
51.255.65.51	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.53	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.61	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
5.29.212.105	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

02-26-2016-21:04:04 to 02-26-2016-22:04:04

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	3
66.102.9.17	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.75.239	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
93.174.91.29	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.91.29	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
59.1.130.84	147.237.76.31	Korea, Republic of	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.246.0.97	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

02-26-2016-21:04:04 to 02-26-2016-22:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.57.180.84	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	29
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	29
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	24
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	24
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	23
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	10
176.13.2.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.81.148	United States	147.237.77.226	www.chamatz.aka.idf.il	drop		drop	6
79.180.50.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.81.148	United States	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
149.88.232.31	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
66.249.81.148	United States	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
66.249.81.148	United States	147.237.77.226	www.chamatz.aka.idf.il	Directory Traversal	directory traversal overflow	monitor	4
5.102.254.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.81.152	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
66.249.81.144	United States	147.237.77.226	www.chamatz.aka.idf.il	drop		drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
66.249.81.144	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
196.217.197.45	Morocco	147.237.77.216	dover.idf.il	drop		drop	4
79.181.59.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.67.221.76	Israel	147.237.77.243	mobile.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
5.28.157.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.81.152	United States	147.237.77.226	www.chamatz.aka.idf.il	drop		drop	3
77.126.90.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.23.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.144.109	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
104.179.24.26	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.210.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.81	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.79.121	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.63.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.162.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.97.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.81.144	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
5.102.254.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.81.152	United States	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.64.165.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.54.183.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
66.249.81.234	United States	147.237.0.15	kosher-kravi.idf.il	Directory Traversal	directory traversal overflow	monitor	2
46.19.85.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
31.210.187.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.81.212	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	2

02-26-2016-21:04:04 to 02-26-2016-22:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.17.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
195.154.173.103	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/mazi	Block	3
85.64.165.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.250.149.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
37.220.115.231	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/☺▫▫	Block	1
85.64.46.32	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.79.235	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
157.55.39.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.75.77.36	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/28/	Block	1
40.77.167.92	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
199.30.24.14	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.81.148	United States	147.237.77.226	www.chamatz.aka.idf.il	URL is Above Root Directory www.chamatz.aka.idf.il/../../images/shared/menustrech.png	Block	1
78.47.62.212	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
66.249.66.33	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf	Block	1
199.30.25.28	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.74.151.149	Slovakia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
66.249.81.218	United States	147.237.77.216	dover.idf.il	Distributed URL is Above Root Directory	Block	1
185.82.200.91		147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
66.249.66.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1613-he/dover.aspx	Block	1
213.57.180.84	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
116.253.140.224	China	147.237.72.156	aman.idf.il	Admin Blocking	Block	1
66.249.81.237	United States	147.237.0.15	kosher-kravi.idf.il	Multiple URL is Above Root Directory from 66.249.81.237	Block	1
37.26.146.182	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
185.82.200.91		147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
84.229.244.112	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.66.40	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1381-he/dover.aspx	Block	1
116.253.140.224	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/admin/login.asp	Block	1

02-26-2016-21:04:04 to 02-26-2016-22:04:04