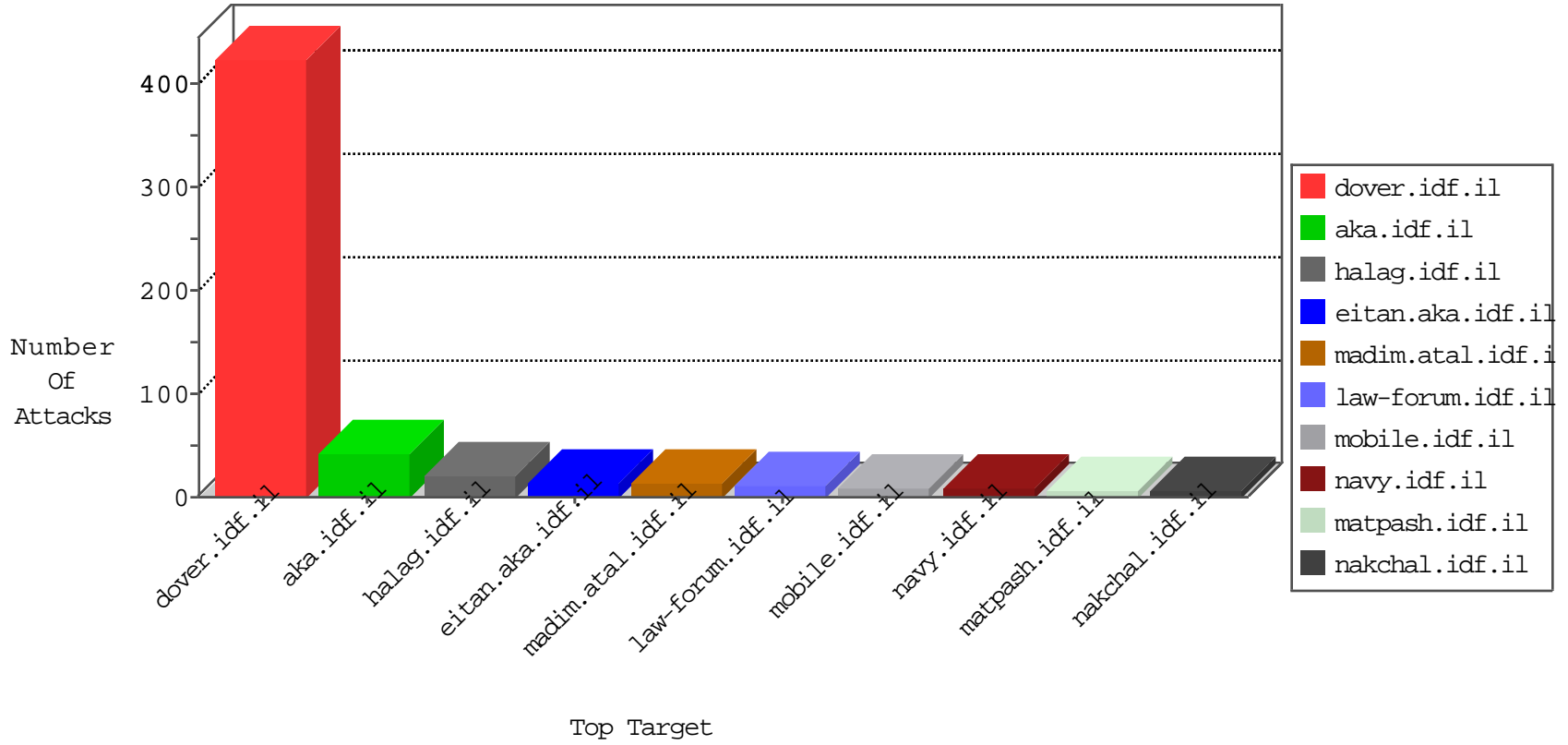


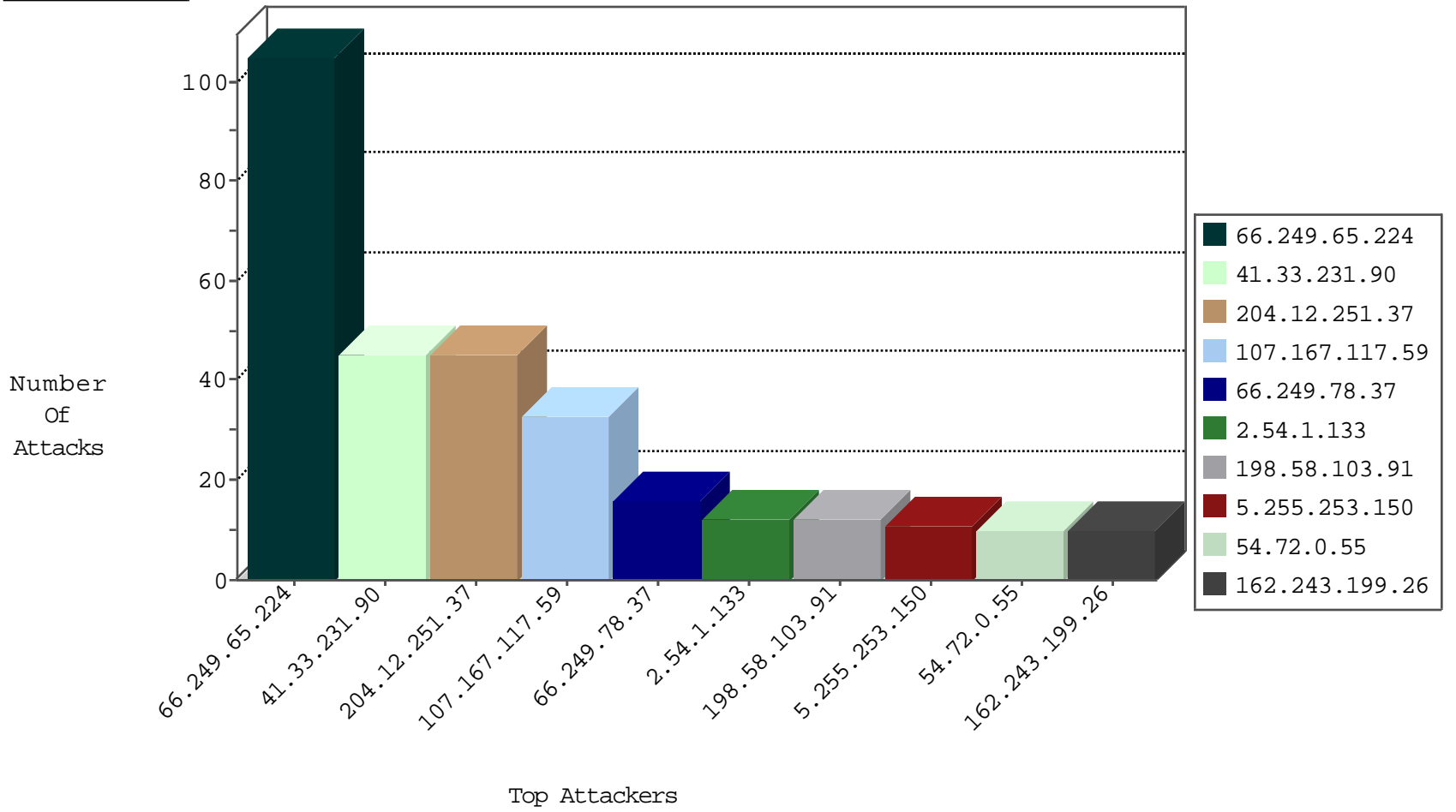
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
37.21.180.127	Russian Federation	147.237.76.198	e.yohanan.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
166.78.205.55	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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
149.78.151.221	147.237.76.31	Israel	nakchal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
169.54.233.118	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.118	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.8	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
23.99.54.247	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.118	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.118	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
66.249.67.240	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
23.99.54.247	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
222.45.213.12	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
169.54.233.118	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	94
204.12.251.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
107.167.117.59	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
66.249.78.37	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
2.54.1.133	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	11
162.243.199.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
95.108.158.152	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
77.126.151.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
82.80.175.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.119	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
5.255.253.158	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.254.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
178.152.247.232	Qatar	147.237.77.19	law-forum.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
2.54.15.120	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
207.46.13.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
64.233.172.155	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
198.58.102.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
82.145.217.167	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
76.114.72.77	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
64.233.172.163	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
64.233.172.171	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.65.151.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.217.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.152	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
207.241.229.193	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	3
66.249.67.79	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.179.119.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
64.236.82.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
87.69.106.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
207.46.13.123	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
64.12.253.130	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
115.31.176.2	Thailand	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
172.56.41.191	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.65.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	7
2.54.18.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.246.136.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.16.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	2
66.249.67.31	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
114.98.228.209	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1058-he/cogat.aspx/trackback/	Block	1
75.102.8.33	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/blog/wp-admin/	Block	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/news/pages/mitshel.aspx	Block	1
209.53.188.210	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
37.211.235.135	Qatar	147.237.77.19	law-forum.idf.il	Distributed Unauthorized URL Access on 147.237.77.19/	Block	1
107.150.55.50	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to /	Block	1
66.249.67.243	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluil/main35cc.html	Block	1
141.212.122.160	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
79.229.205.65	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wordpress/wp-admin/	Block	1
210.224.185.23	Japan	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/old/wp-admin/	Block	1
193.201.224.32	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/shared/usercontrols/headerupper/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.69	Block	1
166.78.9.12	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
216.104.160.96	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp/wp-admin/	Block	1
198.143.138.42	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp-admin/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.55	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/tutimprahim1601201100.aspx	Block	1
176.12.139.119	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
95.30.53.94	Russian Federation	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
202.124.242.10	Australia	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/test/wp-admin/	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/news/pages/siyamilhama.aspx	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
176.12.142.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/adguard-ajax-api/api	Block	1
107.150.43.202	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1
66.249.67.240	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
204.12.251.37	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/usercontrols/headerupper/	Block	1