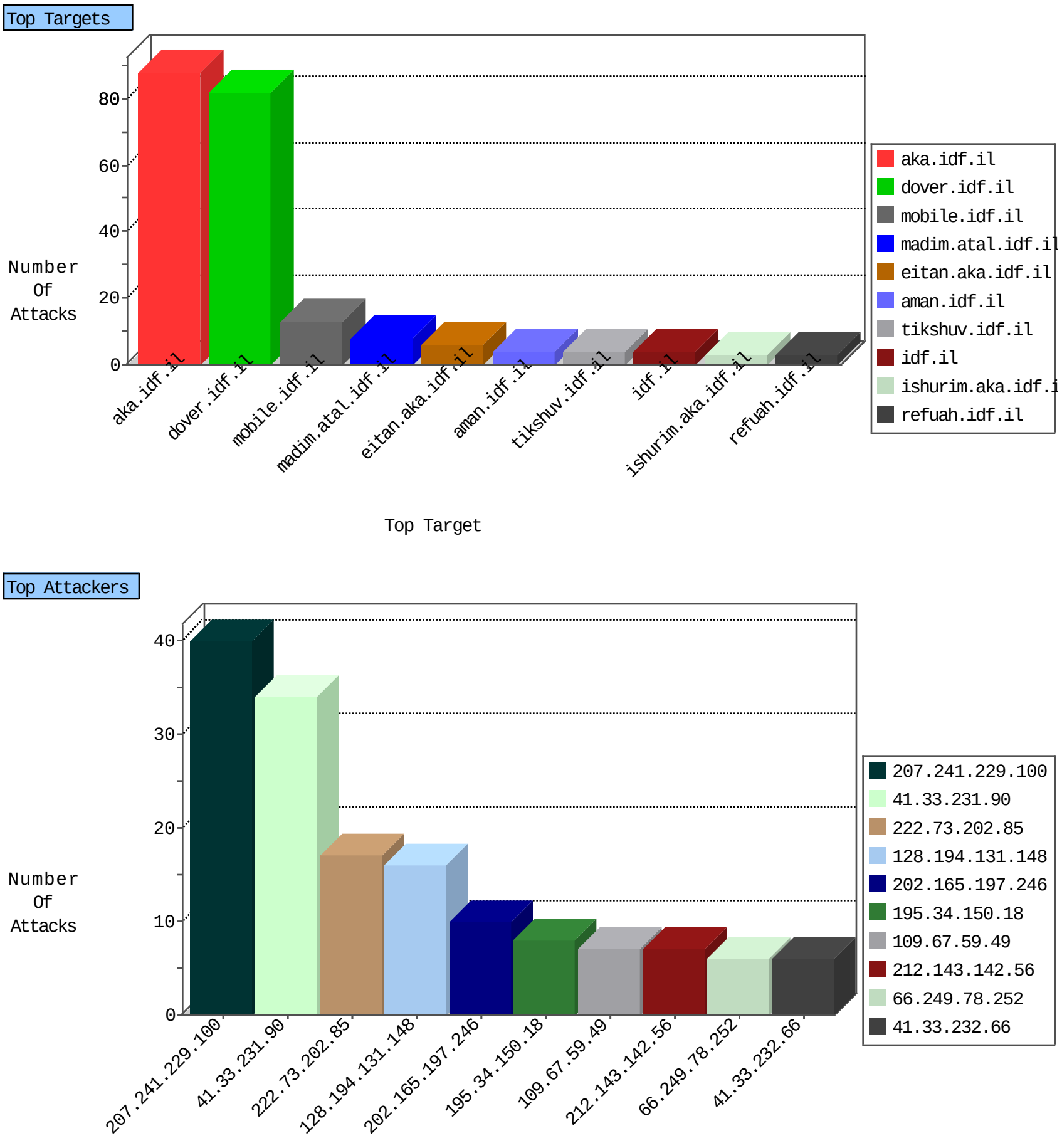
02-07-2016-03:04:07 to 02-07-2016-04:04:07

IDF Under Attack
Daily Report



02-07-2016-03:04:07 to 02-07-2016-04:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.91.28.61	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	drop	1
185.56.28.67	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1

02-07-2016-03:04:07 to 02-07-2016-04:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-07-2016-03:04:07 to 02-07-2016-04:04:07

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
213.244.233.123	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
222.73.202.85	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
183.61.109.189	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
222.73.202.85	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
183.61.109.189	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
222.73.202.85	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
175.143.70.237	147.237.77.205	Malaysia	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
222.73.202.85	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.2	147.237.0.33	Russian Federation	idf.il	ET SCAN NMAP -sS window 1024	1
222.73.202.85	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
222.73.202.85	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.76.30		himush.idf.il	ET SCAN NMAP -sS window 1024	1
213.244.233.123	147.237.0.35		akaws.idf.il	ET SCAN Potential SSH Scan	1
14.145.4.65	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.73.202.85	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
5.199.172.154	147.237.0.33	Lithuania	idf.il	ET SCAN NMAP -sS window 2048	1
222.73.202.85	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
222.73.202.85	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
185.56.28.72	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential SSH Scan	1
222.73.202.85	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
183.61.109.189	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
222.73.202.85	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
175.143.70.237	147.237.77.205	Malaysia	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
222.73.202.85	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
175.143.70.237	147.237.77.205	Malaysia	prisha.idf.il	ET SCAN NMAP -f -sS	1
222.73.202.85	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
93.189.26.18	147.237.77.121	Austria	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
222.73.202.85	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
222.73.202.85	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
213.244.233.123	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	1
5.199.172.154	147.237.0.33	Lithuania	idf.il	ET SCAN NMAP -sS window 4096	1
222.73.202.85	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
213.244.233.123	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
5.199.172.154	147.237.0.33	Lithuania	idf.il	ET SCAN NMAP -f -sS	1
222.73.202.85	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1

02-07-2016-03:04:07 to 02-07-2016-04:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
207.241.229.100	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
202.165.197.246	Papua New Guinea	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.67.59.49	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.252	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
128.194.131.148	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
66.249.78.170	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.45.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.217.10	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.30.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
40.77.167.105	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.80	United States	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.194.131.148	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
37.46.39.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
103.14.88.99	Papua New Guinea	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
68.194.87.253	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
74.125.93.100	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
220.181.108.163	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
149.78.184.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
81.169.237.146	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
46.121.140.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
202.165.197.246	Papua New Guinea	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
81.169.237.146	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	1
202.165.197.246	Papua New Guinea	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
128.194.131.148	United States	147.237.72.156	aman.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
79.181.64.160	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.224	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
81.169.237.146	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1

02-07-2016-03:04:07 to 02-07-2016-04:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
128.194.131.148	United States	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 128.194.131.148	Block	7
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	4
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	3
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	3
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	3
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	3
5.29.93.171	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
85.214.155.116	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	2
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	2
188.143.232.34	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	1
111.13.102.5	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/3192.pdf	Block	1
2.54.33.154	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
204.124.83.130	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.10.104.240	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.245	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SearchText in eitan.aka.idf.il/938-he/eitan.aspx	None	1
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58436	Block	1
128.194.131.148	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
204.124.83.130	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/y1cebowm67a	Block	1
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
176.10.104.240	Switzerland	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 176.10.104.240	Block	1
66.249.78.245	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SortDir in eitan.aka.idf.il/938-en/eitan.aspx	None	1
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	1
46.165.230.5	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.10.104.240	Switzerland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/src="http:/www.youtube.com/v/0mwqtcld1fe	Block	1
128.194.131.148	United States	147.237.72.166	aka.idf.il	NULL Character in Method	Block	1
66.249.64.191	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
178.255.215.87	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
109.67.59.49	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59331&docid=73449	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59268&docid=65421	Block	1
176.10.104.240	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	1

02-07-2016-03:04:07 to 02-07-2016-04:04:07