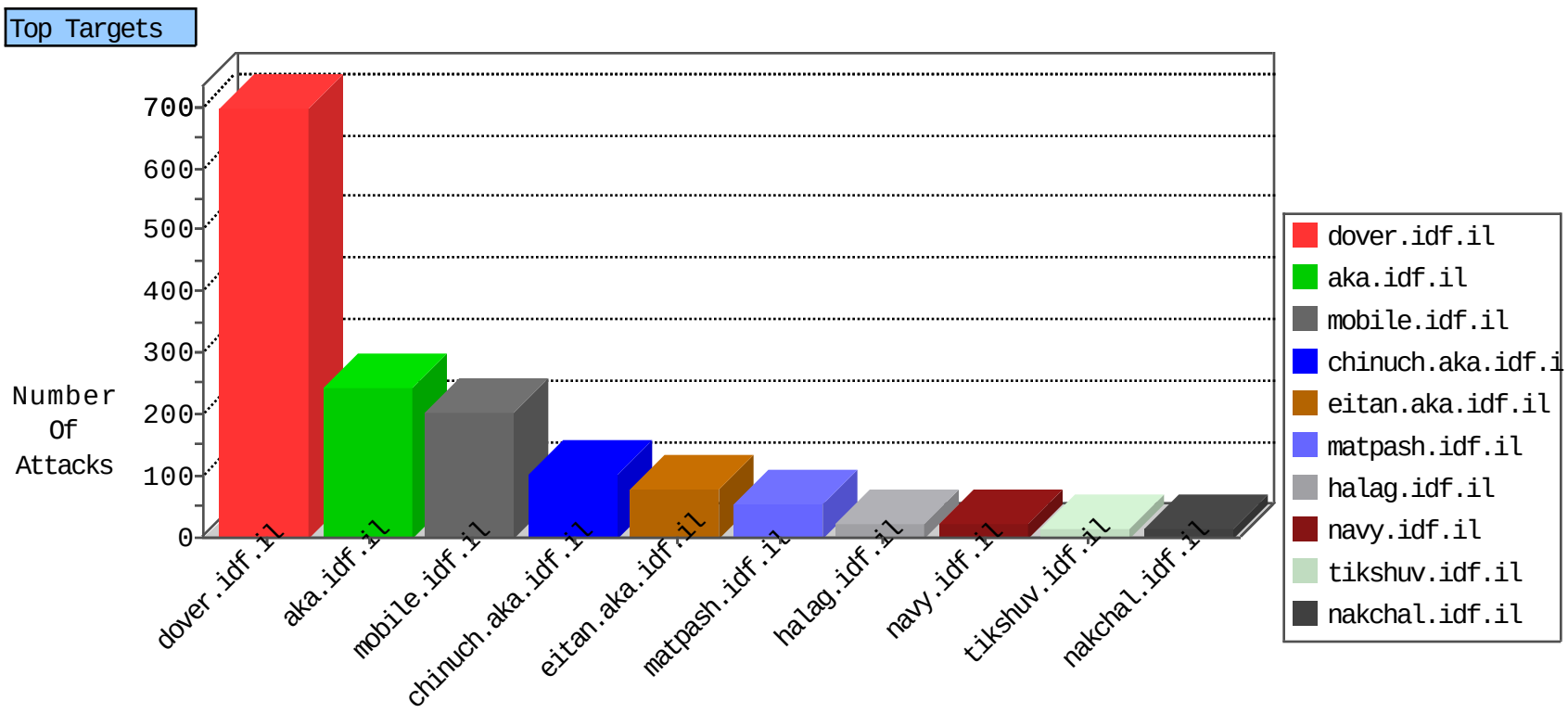
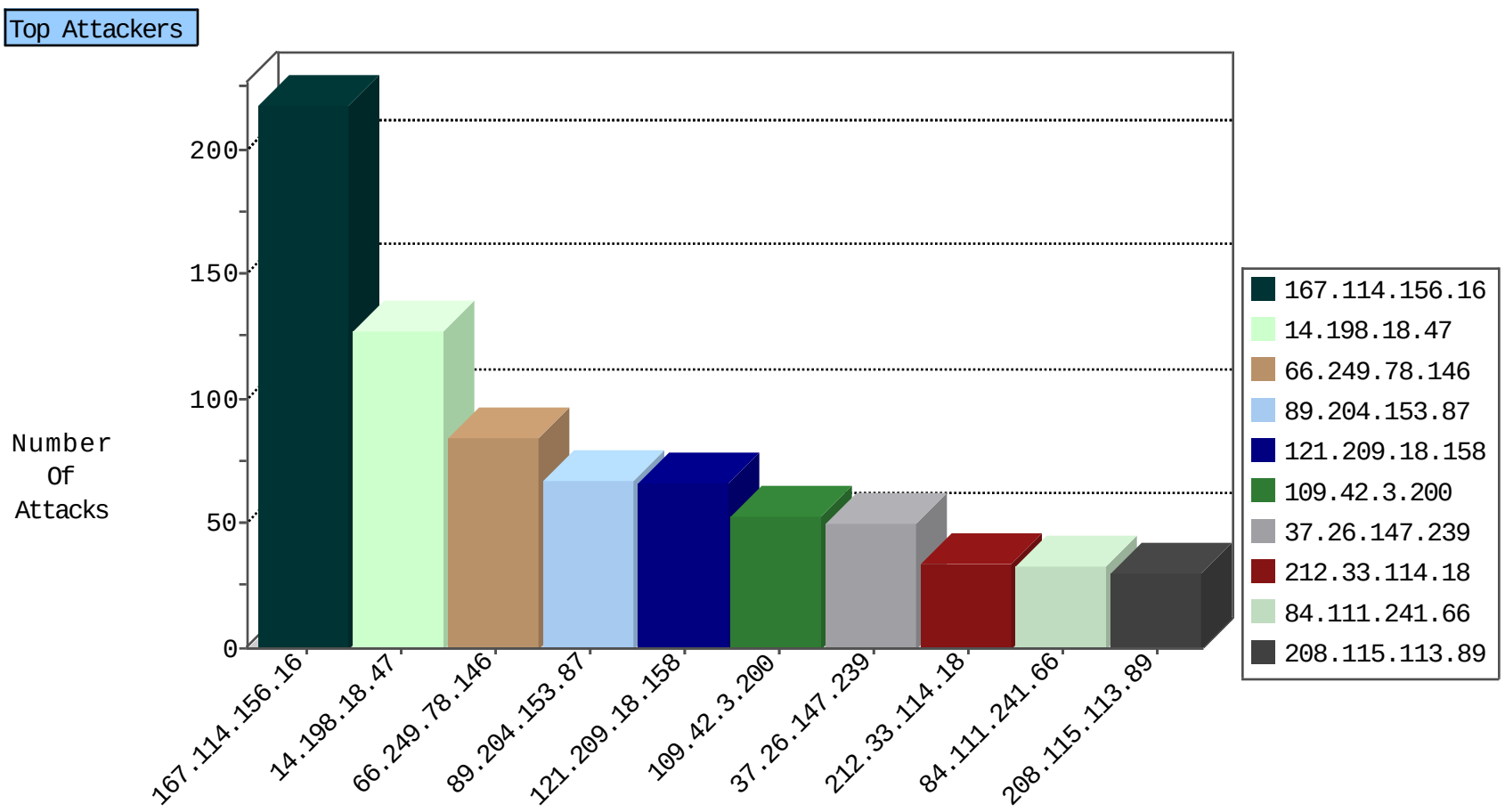
04-29-2016-13:04:08 to 04-29-2016-14:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-29-2016-13:04:08 to 04-29-2016-14:04:08

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	HTTP-POST-Segmented-DoS	dest-reset	9486
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2856
87.69.175.117	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	101
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	5
212.143.254.66	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
125.25.225.113	Thailand	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

04-29-2016-13:04:08 to 04-29-2016-14:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
70.68.224.173	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
198.143.180.166	United States	147.237.77.19	law-forum.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

04-29-2016-13:04:08 to 04-29-2016-14:04:08

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
80.82.78.38	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
193.227.34.78	147.237.76.44	Egypt	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
58.218.204.211	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
147.83.130.22	147.237.77.216	Spain	dover.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
193.227.34.78	147.237.76.44	Egypt	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.211	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
174.37.194.144	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -f -sS	1
89.248.167.131	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1
193.227.34.78	147.237.76.44	Egypt	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1

04-29-2016-13:04:08 to 04-29-2016-14:04:08

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	84
89.204.153.87	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
109.42.3.200	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	53
121.209.18.158	Australia	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
37.26.147.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
212.33.114.18	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
84.111.241.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
46.121.247.153	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
82.166.119.97	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
188.120.148.107	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
107.167.107.11	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
185.32.179.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
121.209.18.158	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
176.13.14.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.177.68.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
157.55.39.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.32.179.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
70.39.186.218	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.254.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.53.12.61	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.84.102	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
79.177.39.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.78	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
5.28.189.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
182.118.20.214	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
93.172.242.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.196.160	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
14.198.18.47	Hong Kong	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.120.76.203	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.39.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
130.206.88.106	Spain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.147.239	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence		monitor	4
8.37.227.70	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.22.134.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.99.1.198	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

04-29-2016-13:04:08 to 04-29-2016-14:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
14.198.18.47	Hong Kong	147.237.76.147	chinuch.aka.idf.i	Distributed PHP Attempt	Block	41
14.198.18.47	Hong Kong	147.237.76.147	chinuch.aka.idf.i	Multiple Unauthorized URL Access from 14.198.18.47	Block	41
14.198.18.47	Hong Kong	147.237.76.147	chinuch.aka.idf.i	Distributed Admin Blocking	Block	19
79.176.56.72	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	7
82.166.119.97	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
37.26.147.239	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
62.0.70.140	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/801-he/patzar.aspx	Block	5
14.198.18.47	Hong Kong	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 14.198.18.47	Block	4
14.198.18.47	Hong Kong	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	3
79.177.68.5	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.179.201.171	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	3
69.30.223.170	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
85.64.163.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.172.242.32	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
80.246.139.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.119.113.162	Ukraine	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	2
14.198.18.47	Hong Kong	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 14.198.18.47	Block	2
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	2
93.173.10.83	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	2
14.198.18.47	Hong Kong	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
14.198.18.47	Hong Kong	147.237.76.42	refuah.idf.il	PHP Attempt	Block	2
79.176.56.72	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.176.56.72	Block	2
14.198.18.47	Hong Kong	147.237.0.34	tikshuv.idf.il	Multiple Admin Blocking from 14.198.18.47	Block	2
207.46.13.137	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
69.30.223.170	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 69.30.223.170	Block	2
79.176.56.72	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	2
109.67.200.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.254	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.177.39.200	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.253.224.124	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.229.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/smalim/html/4.asp	Block	1
85.65.90.105	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
14.198.18.47	Hong Kong	147.237.76.42	refuah.idf.il	Multiple Admin Blocking from 14.198.18.47	Block	1
79.179.201.171	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
74.82.47.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
1.39.21.135	India	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/mobile	Block	1
188.120.148.107	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
93.173.10.83	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 93.173.10.83	Block	1
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/size100x0/2969.jpg	Block	1
14.198.18.47	Hong Kong	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
120.146.153.24	Australia	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/changelog.txt	Block	1
69.30.223.170	United States	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
46.119.113.162	Ukraine	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 46.119.113.162	Block	1
86.134.233.73	United Kingdom	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
2.53.12.61	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	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
84.111.39.77	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
17.142.159.155	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/apple-app-site-association	Block	1
79.177.136.159	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.177.136.159	Block	1

04-29-2016-13:04:08 to 04-29-2016-14:04:08