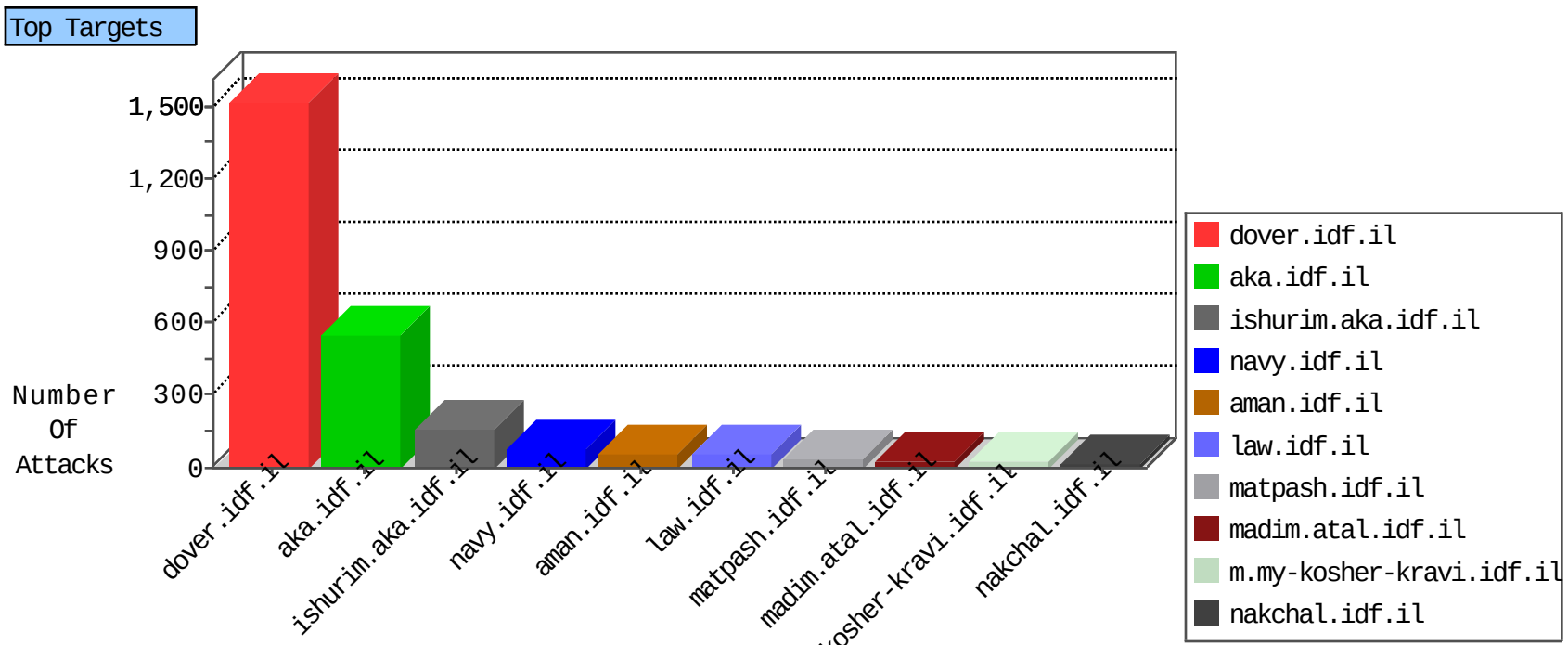
10-20-2015-08:04:02 to 10-20-2015-09:04:02

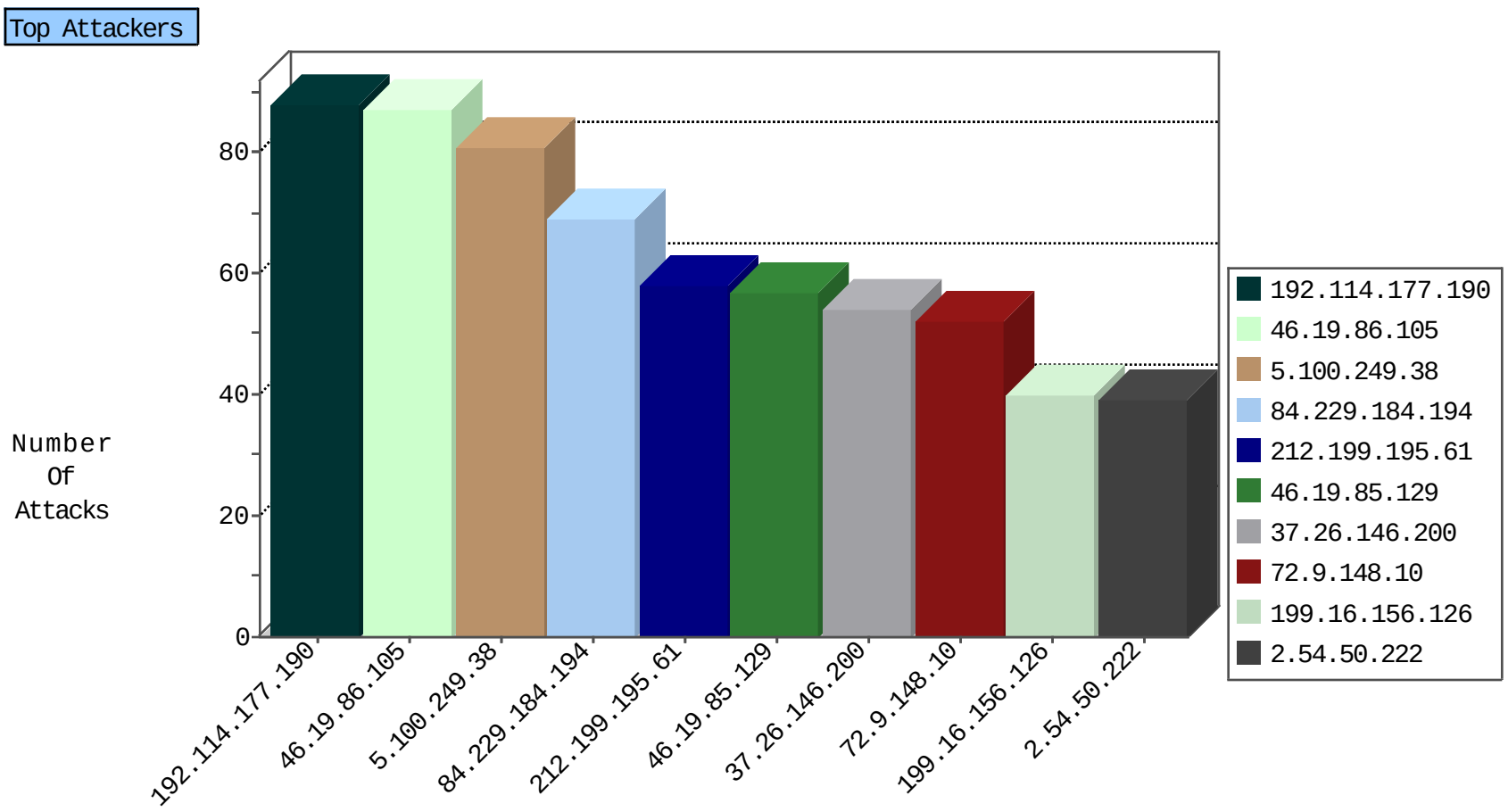
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-20-2015-08:04:02 to 10-20-2015-09:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.105	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	125
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
2.54.1.40	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
62.219.137.64	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
192.118.48.248	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
2.54.1.40	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
2.54.177.69	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	7
46.19.86.184	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
54.187.55.213	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
188.70.0.157	Kuwait	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
132.74.209.225	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
91.199.69.254	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
104.129.192.59	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
192.168.1.102		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
91.135.102.164	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
41.250.209.222	Morocco	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
213.151.32.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
93.174.93.181	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
2.54.0.73	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
91.135.102.164	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
5.22.129.76	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-20-2015-08:04:02 to 10-20-2015-09:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.29.202.206	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6

10-20-2015-08:04:02 to 10-20-2015-09:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	11
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
123.196.116.66	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
111.93.198.54	147.237.76.44	India	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
41.190.132.132	147.237.72.14	Uganda	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
5.148.157.229	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
168.187.177.203	147.237.8.50	Kuwait	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
123.196.116.66	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
78.163.250.117	147.237.76.38	Turkey	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-20-2015-08:04:02 to 10-20-2015-09:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.114.177.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
212.199.195.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
84.229.184.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
37.26.146.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
46.19.85.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
58.8.5.14	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
212.76.127.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
192.0.81.55	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
212.29.194.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
100.100.102.12		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.19.86.105	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	22
37.142.245.33	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
85.250.225.75	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.184	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
192.0.100.59	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
62.219.124.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
192.0.81.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
62.219.137.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
176.13.11.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
194.90.125.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.182.5.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
194.114.146.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
132.68.23.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
45.33.117.254		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
2.54.1.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.101.2.201	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
5.100.249.38	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
45.33.114.177		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
79.178.105.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
81.218.175.31	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
109.66.21.47	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
31.168.196.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.19.86.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
72.218.35.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.52.191.48	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.118.48.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
31.168.196.242	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
45.33.26.180		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8

10-20-2015-08:04:02 to 10-20-2015-09:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	52
5.100.249.38	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	39
199.16.156.126	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.16.156.126	Block	39
213.151.57.156	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	39
2.54.50.222	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	39
5.100.249.38	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	26
95.86.67.12	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/default.aspx/	Block	26
199.16.156.124	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/4/size220x0/17374.jpg	Block	26
122.96.31.66	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	13
84.228.238.223	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	13
203.109.98.107	India	147.237.0.34	tikshuv.idf.il	Parameter Type Violation lang in www.tikshuv.idf.il/modules/forums/forumslist.aspx	Block	13
66.249.64.3	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	13
185.32.179.14	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	13
85.250.18.153	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	13
66.249.67.210	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/228-he/faq.aspx	Block	13
46.19.85.248	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	13
199.16.156.125	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/4/size220x0/17374.jpg	Block	13
147.236.113.1	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	13
84.228.238.223	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 84.228.238.223	None	13
207.46.13.88	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
66.249.64.17	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	13
185.32.179.107	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	13
93.172.21.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1	Block	13
46.19.85.255	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	13
162.243.188.75	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to /	Block	13
2.52.189.106	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.189.106	Block	13
84.229.184.194	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	13
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
41.215.151.246	Swaziland	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.215.151.246	Block	13
192.116.95.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
199.59.148.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/4/size220x0/17374.jpg	Block	13
46.19.86.216	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	13
168.235.198.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clientscripts/ui/ui.datepickex²Ö³Ö´	Block	13
2.54.26.225	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
85.64.157.193	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
217.194.206.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
41.215.151.246	Swaziland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	13
192.116.102.76	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	13
109.66.178.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	13
82.166.140.117	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1141-he/navy.aspx/	Block	13
199.59.148.211	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/4/size220x0/17374.jpg	Block	13
62.219.165.164	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl54.y in www.aka.idf.il/main/sachar/payslips.aspx	None	13
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/kkkkkkk=cd07c66ckkkkkkk_cd07c66c	Block	13
85.250.18.153	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pniasubmittedsuccessfully.aspx	None	13
66.249.67.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	13
45.57.139.42		147.237.0.19	madim.atal.idf.il	Parameter Type Violation ReturnUrl in madim.atal.idf.il/login.aspx	Block	13

10-20-2015-08:04:02 to 10-20-2015-09:04:02