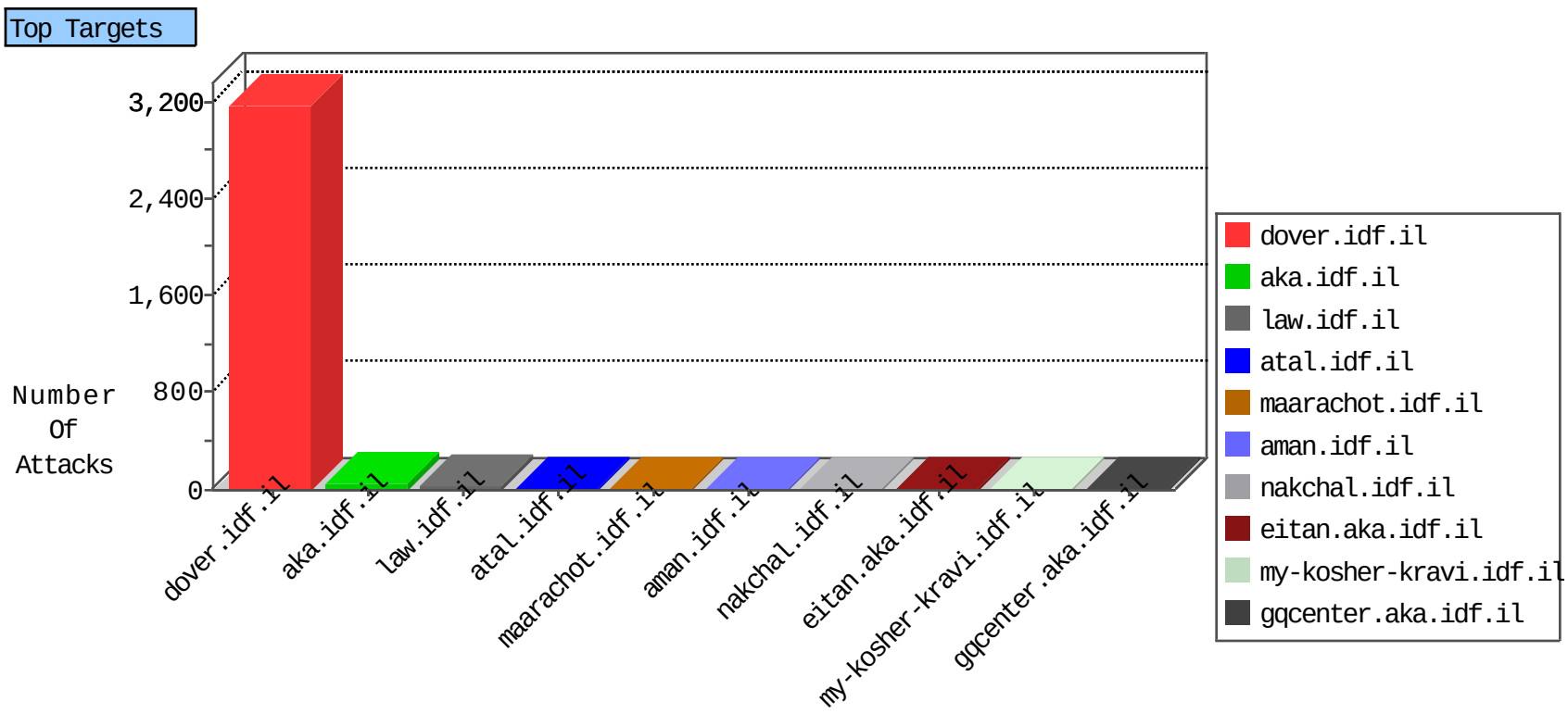
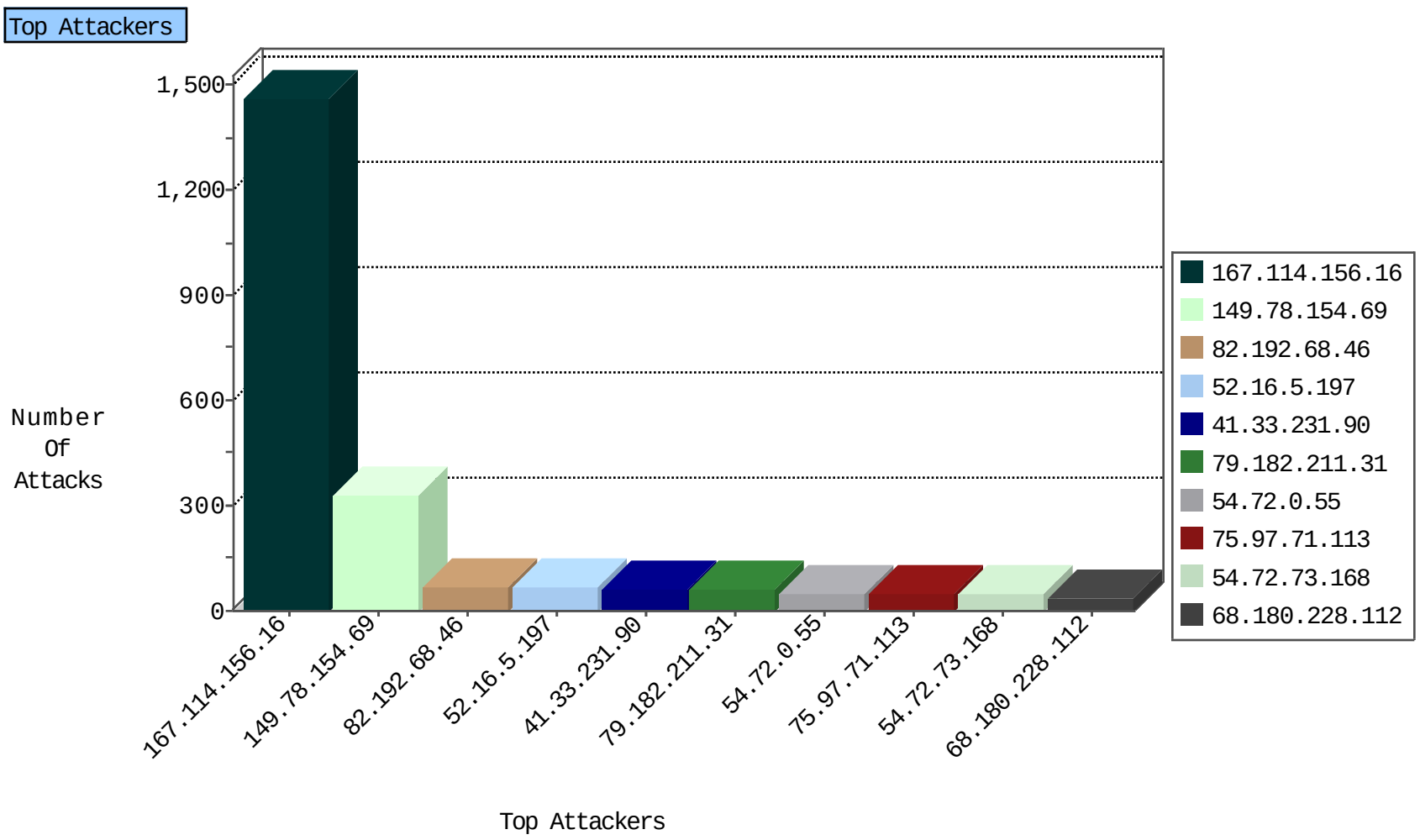
11-09-2015-04:04:07 to 11-09-2015-05:04:07

IDF Under Attack Daily Report





11-09-2015-04:04:07 to 11-09-2015-05:04:07

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	DOS-Tool-SwitchbladG	dest-reset	2525
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	339
2.54.170.34	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
81.218.234.122	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
178.121.254.193	Belarus	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
81.218.235.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

11-09-2015-04:04:07 to 11-09-2015-05:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.8.66.129	Russian Federation	147.237.72.166	aka.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	4
5.8.66.129	Russian Federation	147.237.77.233	atal.idf.i	20086: HTTP: Muieblackcat Security Scanner	Block	3
5.8.66.129	Russian Federation	147.237.72.166	aka.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

11-09-2015-04:04:07 to 11-09-2015-05:04:07

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	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
221.239.192.203	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
178.151.50.125	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
111.93.198.54	147.237.76.148	India	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
103.232.35.46	147.237.72.156	Hong Kong	aman.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
103.232.35.46	147.237.72.156	Hong Kong	aman.idf.il	ET SCAN NMAP -f -sS	1
84.21.203.130	147.237.0.33	Bulgaria	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.233.47.60	147.237.76.31	Iran, Islamic Republic of	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
111.93.198.54	147.237.76.148	India	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
111.93.198.54	147.237.76.148	India	gqcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
103.232.35.46	147.237.72.156	Hong Kong	aman.idf.il	ET SCAN NMAP -sS window 2048	1
45.55.227.109	147.237.0.16		my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
94.23.247.219	147.237.76.44	France	e.refuah.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
40.115.58.160	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.77.19		law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
5.8.66.129	147.237.72.166	Russian Federation	aka.idf.il	ET WEB_SERVER Muieblackcat scanner	1
59.45.79.117	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1

11-09-2015-04:04:07 to 11-09-2015-05:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	332
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	68
79.182.211.31	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	63
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	62
75.97.71.113	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
66.249.88.91	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
166.137.126.34	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
209.6.187.230	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
71.90.130.114	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
66.249.88.101	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
66.249.65.231	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
131.253.25.166	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
208.115.113.89	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
207.46.13.169	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
66.249.88.81	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
45.219.110.154	Uruguay	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	16
109.160.221.93	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
207.46.13.107	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
82.80.25.221	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
66.249.65.224	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
185.19.194.100	Kazakstan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
173.84.92.42	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
188.165.15.14	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
198.58.103.92	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
198.58.103.91	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
207.46.13.76	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
41.43.18.69	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
162.247.90.12	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
79.182.129.89	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	9
66.249.65.238	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
129.184.84.40	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
37.26.146.223	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
58.246.193.142	China	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
2.54.170.34	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	8
66.249.65.238	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
81.218.235.10	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7

11-09-2015-04:04:07 to 11-09-2015-05:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.210.23.174	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 54.210.23.174	Block	5
66.249.69.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/112935.pdf	Block	1
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcemen!s/20o	Block	1
45.55.75.174		147.237.76.30	himush.idf.il	Distributed Unauthorized URL Access on /	Block	1
167.88.10.196	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.cloud.ph/	Block	1
95.86.87.167	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
66.249.67.85	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/mobile/	Block	1
159.203.81.101	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
45.55.75.174		147.237.76.39	mobile.meitav.idf.il	Distributed Unauthorized URL Access on /	Block	1
184.105.139.68	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	1
104.236.18.52		147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on /	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
54.210.23.174	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
159.203.81.101	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	1
66.249.79.31	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
45.55.227.109		147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
184.105.247.196	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
129.184.84.40	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
159.203.81.101	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
68.180.229.27	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to chimush.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
45.55.227.109		147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to /	Block	1
198.20.69.74	United States	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/	Block	1
144.76.104.83	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 144.76.104.83	Block	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
159.203.81.101	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on /	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1117-he/nakhal.aspx	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
45.55.227.109		147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /	Block	1
144.76.104.83	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/main/	Block	1

11-09-2015-04:04:07 to 11-09-2015-05:04:07