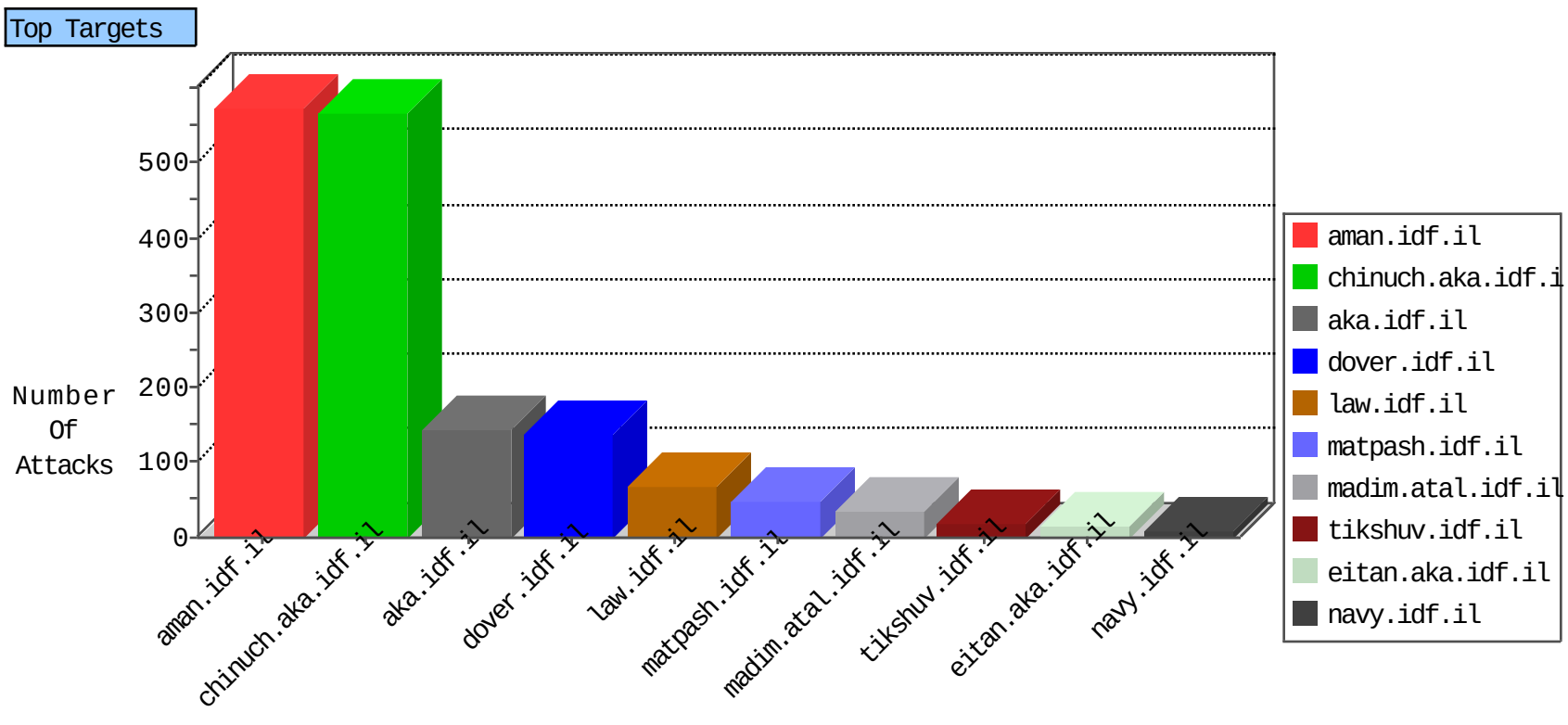
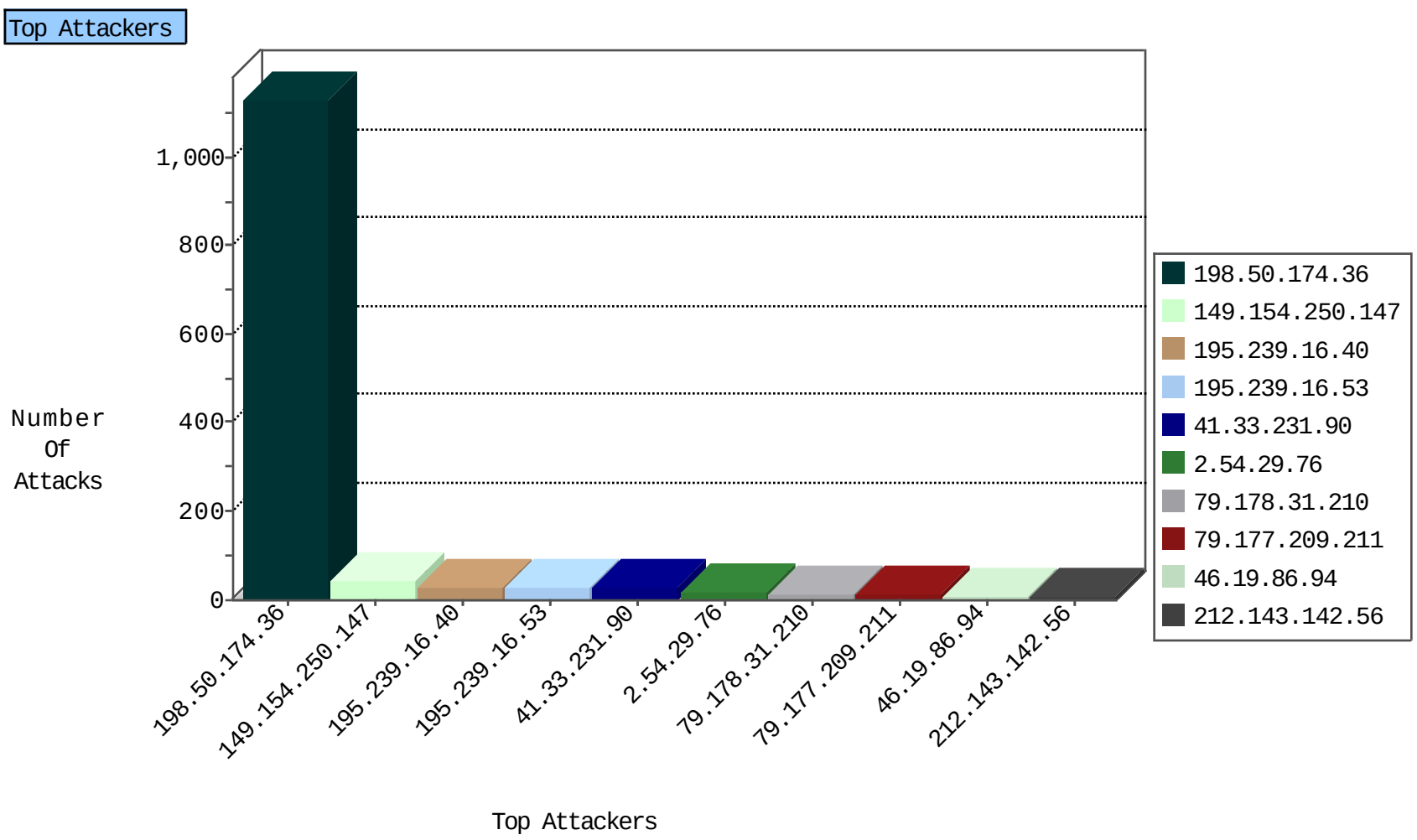
02-04-2016-23:04:09 to 02-05-2016-00:04:09

IDF Under Attack
Daily Report





02-04-2016-23:04:09 to 02-05-2016-00:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
146.185.239.100	Russian Federation	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
198.20.69.98	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
66.249.81.206	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1

02-04-2016-23:04:09 to 02-05-2016-00:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.201	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
151.80.31.112	Italy	147.237.0.15	kosher-kravi.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-04-2016-23:04:09 to 02-05-2016-00:04:09

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
66.249.81.240	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sA (2)	4
188.152.234.175	147.237.77.216	Italy	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	2
112.196.49.101	147.237.76.31	India	nakchal.idf.il	ET SCAN NMAP -f -sS	1
80.82.64.37	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
189.234.56.9	147.237.0.17	Mexico	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.196.49.101	147.237.76.31	India	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
104.128.144.131	147.237.8.46	Canada	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
46.151.52.161	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

02-04-2016-23:04:09 to 02-05-2016-00:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
198.50.174.36	Canada	147.237.72.156	aman.idf.il	SYN Attack		reject	325
198.50.174.36	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	304
198.50.174.36	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	190
198.50.174.36	Canada	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	144
198.50.174.36	Canada	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	96
198.50.174.36	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	71
149.154.250.147	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	24
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	24
79.177.209.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.81.217	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.65.147.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.186.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.2.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
5.102.254.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
185.3.146.233	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.182.192.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
190.208.62.245	Chile	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
179.218.50.153	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.180.111.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.102.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.167.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.224.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.184.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.17.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.140.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.237.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
64.246.165.200	United States	147.237.77.74	law.idf.il	Header Rejection	header rejection pattern found in request	monitor	3
79.177.145.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.124.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.144.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.162.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.211	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
66.249.69.85	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
87.68.148.99	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
195.239.16.40	Russian Federation	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.19.85.111	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

02-04-2016-23:04:09 to 02-05-2016-00:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.29.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
79.178.31.210	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
109.253.145.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
185.3.144.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.127.240.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.183.140.108	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.183.140.108	Block	2
46.238.247.31	Poland	147.237.77.74	law.idf.il	PHP Attempt	Block	2
46.19.85.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.238.247.31	Poland	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
46.19.86.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.204.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
117.78.13.18	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/894-he	Block	1
46.19.86.85	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.51.16.133	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
84.111.61.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/expand.js	Block	1
157.55.39.65	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/size220x0/sip_storage	Block	1
41.250.38.45	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
109.160.194.110	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$1 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/moreinfo/tichnun.yosh@gmail.com	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/datepicker.css	Block	1
124.123.21.71	India	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
84.228.8.138	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$20 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
66.249.74.106	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to chimush.atal.idf.il/templates/news/null	Block	1
157.55.39.173	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/elram	Block	1
82.118.236.3	Bulgaria	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
185.32.179.70	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$42 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/scroller/skin.css	Block	1
124.123.21.71	India	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
37.142.68.7	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
79.179.155.153	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
176.13.6.182	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
109.253.203.92	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
84.108.7.227	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1
149.78.185.96	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
54.251.144.191	Singapore	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /	Block	1
37.142.68.7	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
95.86.66.230	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
79.180.200.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	1

02-04-2016-23:04:09 to 02-05-2016-00:04:09