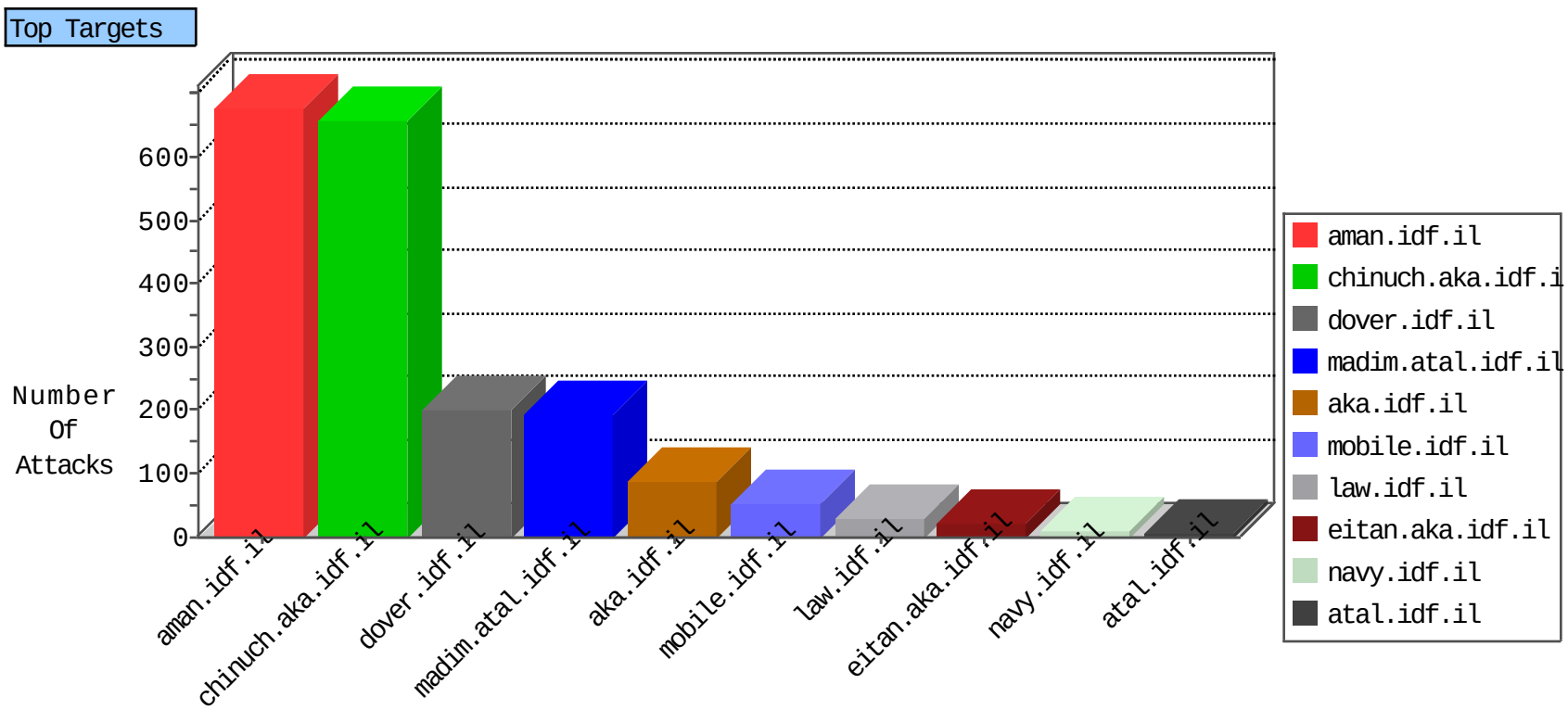
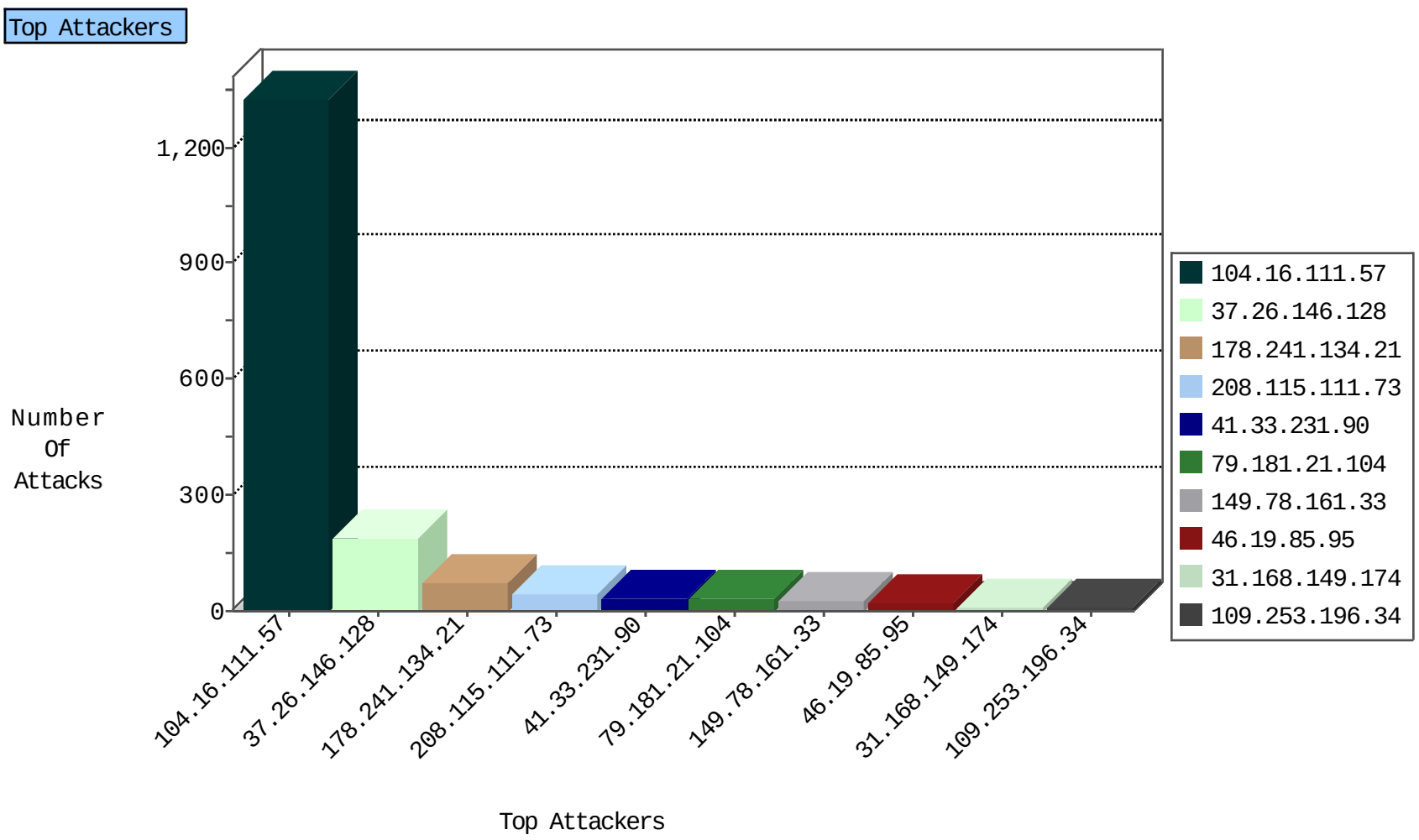
02-06-2016-00:04:06 to 02-06-2016-01:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-06-2016-00:04:06 to 02-06-2016-01:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	22
66.249.78.31	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	14
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
134.147.203.115	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	2
54.244.22.103	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1

02-06-2016-00:04:06 to 02-06-2016-01:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.121.185	United Kingdom	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1

02-06-2016-00:04:06 to 02-06-2016-01:04:06

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
37.26.146.128	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
31.211.102.129	147.237.8.24	Russian Federation	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
82.117.208.243	147.237.77.243		mobile.idf.il	ET SCAN NMAP -sS window 1024	1
69.30.205.130	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.65	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
46.148.22.26	147.237.77.216	Lithuania	dover.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.170	United States	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.148.22.26	147.237.76.177	Lithuania	ncore.idf.il	ET SCAN Potential SSH Scan	1
123.193.66.198	147.237.76.30	Taiwan	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
36.249.203.128	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.189.26.18	147.237.76.197	Austria	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
69.30.205.130	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
69.30.205.130	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.64	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.148.22.26	147.237.77.243	Lithuania	mobile.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.148.22.26	147.237.77.61	Lithuania	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
93.189.26.18	147.237.77.216	Austria	dover.idf.il	ET SCAN NMAP -sS window 1024	1

02-06-2016-00:04:06 to 02-06-2016-01:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
104.16.111.57	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	668
104.16.111.57	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	652
79.181.21.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
149.78.161.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
178.241.134.21	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	19
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
178.241.134.21	Turkey	147.237.77.216	dover.idf.il	SYN Attack		reject	14
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	13
178.241.134.21	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
178.241.134.21	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
208.115.111.73	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	12
178.241.134.21	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
46.19.85.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
31.168.149.174	Israel	147.237.77.243	mobile.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	7
79.179.216.105	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.245	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
66.249.65.122	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.187.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.196.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.186.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.78.233	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.48	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
5.22.131.66	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
149.88.145.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
31.210.186.143	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.156.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.160.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
104.16.111.57	United States	147.237.72.156	aman.idf.il	SYN Attack		reject	2
213.8.204.8	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
23.101.61.176	Ireland	147.237.72.156	aman.idf.il	drop	SAM rule	drop	2
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	2
46.19.86.222	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.148.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
115.230.124.164	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
87.69.217.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
192.169.244.12	United States	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
31.210.186.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.54.57.33	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.73	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.102.254.109	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
87.69.217.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
223.73.103.184	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1

02-06-2016-00:04:06 to 02-06-2016-01:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
37.26.146.128	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.146.128	Block	92
92.114.82.10	Romania	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 92.114.82.10	Block	5
2.52.25.167	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.52.25.167	Block	4
61.113.74.231	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	4
2.52.25.167	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
109.253.196.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	2
37.46.38.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	2
77.127.240.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
17.138.55.213	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	2
130.193.189.131	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
77.221.7.49	Bosnia and Herzegovina	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.78.170	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter PageNum in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
46.236.24.54	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
188.143.232.70	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	1
92.114.82.10	Romania	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
197.38.144.100	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.74.104	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/111572.pdf	Block	1
149.78.65.243	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.180.198.210	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.245	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in eitan.aka.idf.il/1001-en/eitan.aspx	None	1
47.88.13.149	Canada	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
104.175.7.38	United States	147.237.72.167	ishurim.aka.idf.il	Too Many 404: Response Code per Session	Block	1
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	1
217.73.208.111	Italy	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 217.73.208.111	Block	1
66.249.74.106	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/3/107653.pdf	Block	1
85.64.195.193	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$96 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.78.245	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in eitan.aka.idf.il/1085-en/eitan.aspx	None	1
47.88.13.149	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/plus/flink.php	Block	1
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=62217&docid=76712	Block	1
104.175.7.38	United States	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 104.175.7.38	Block	1
2.52.151.156	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
217.73.208.111	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.74.108	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/3/109103.pdf	Block	1
46.117.216.140	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19650-he/kkkkkkk=fa4e71f5kkkkkkk_fa4e71f5	Block	1
85.64.195.193	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.78.245	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in eitan.aka.idf.il/999-en/eitan.aspx	None	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xyzzy	Block	1
77.221.7.49	Bosnia and Herzegovina	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal	Block	1
46.236.24.52	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
185.20.4.220	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
195.138.85.250	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/sendtofriend.aspx?&amp	Block	1
66.249.65.138	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

02-06-2016-00:04:06 to 02-06-2016-01:04:06