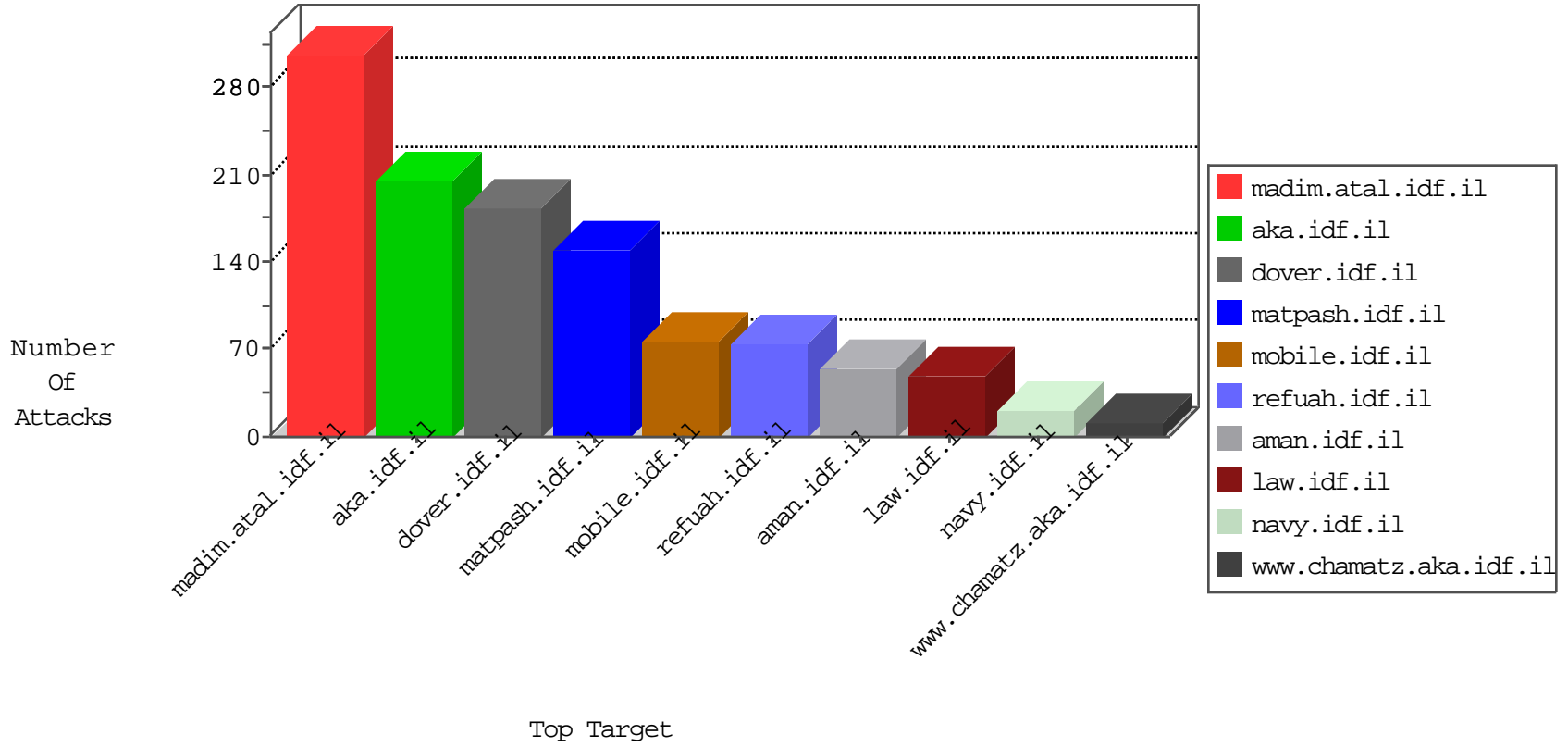


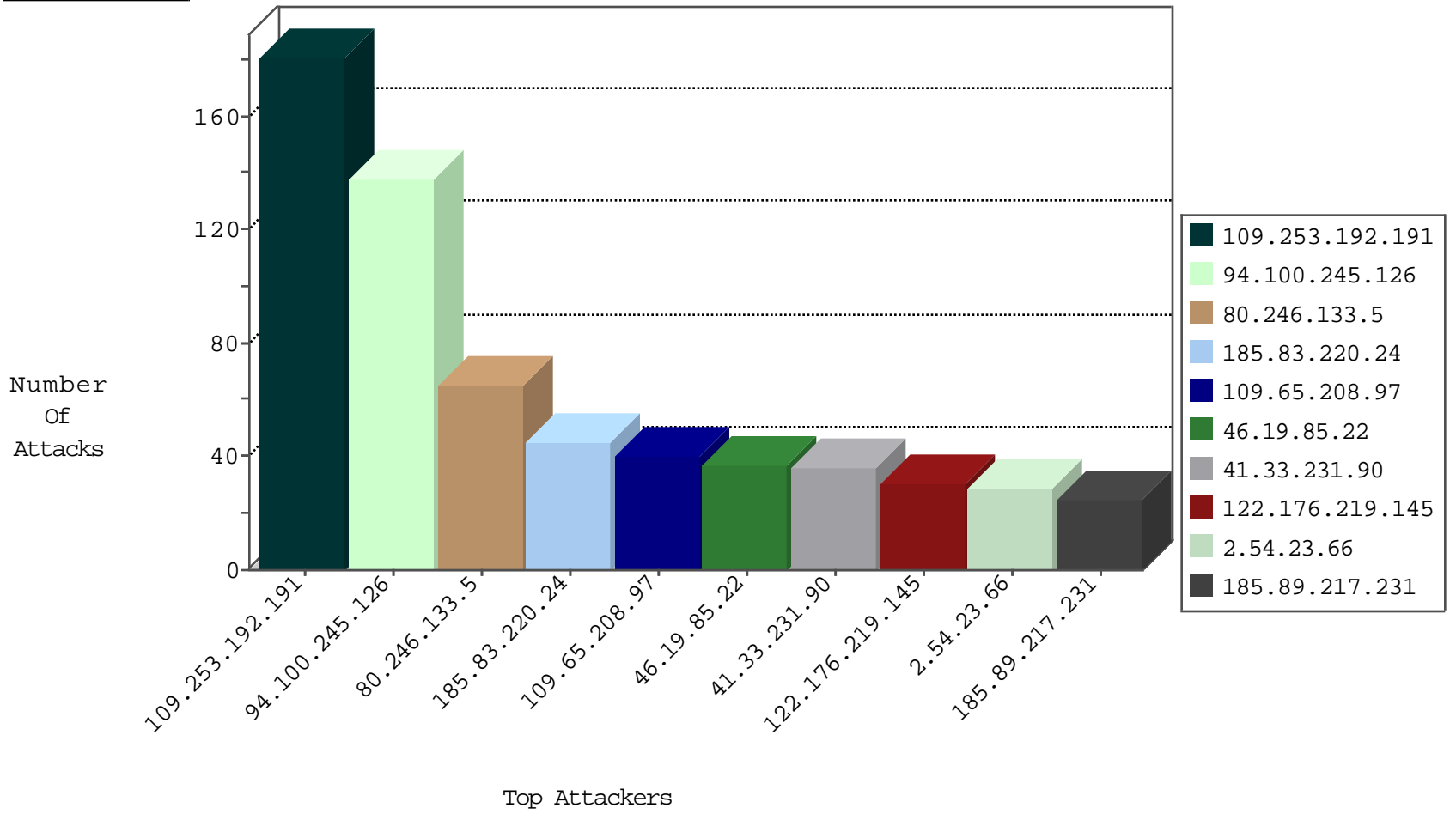
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.206.82	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
95.185.96.142	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
141.212.122.81	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
94.102.48.195	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.82	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
104.207.128.23	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1

02-05-2016-10:04:07 to 02-05-2016-11:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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
91.238.82.41	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
89.248.172.201	147.237.76.148	Netherlands	ggcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.172.201	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.230.148.132	147.237.76.176	Germany	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
209.126.116.147	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
201.235.215.254	147.237.77.178	Argentina	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
89.248.172.201	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.172.201	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.149.222.239	147.237.76.30	Germany	himush.idf.il	ET SCAN NMAP -sS window 1024	1
5.230.148.132	147.237.76.176	Germany	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
209.126.116.147	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
201.235.215.254	147.237.77.178	Argentina	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.100.245.126	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	137
80.246.133.5	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	64
109.65.208.97	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	35
46.19.86.8	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
122.176.219.145	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.86.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
185.89.217.231		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	16
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.172.96.232	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
141.0.15.183	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
185.89.217.227		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
122.176.219.145	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	8
119.188.4.3	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	8
2.52.144.244	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.226	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.190.67	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.78.5	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.24.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.0.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.67	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.205	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.108.168.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.176.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.187.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.86.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
122.176.219.145	India	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.141	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
46.19.85.18	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.176.8.181	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.26.149.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
67.195.192.148	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
188.120.148.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.178.101.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.52.143.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.171.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.104.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.24.155	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
84.228.191.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.179.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
194.90.167.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.192.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
109.253.192.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
185.83.220.24		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
46.19.85.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
2.54.23.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
109.64.148.230	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.64.148.230	Block	7
109.253.192.191	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 109.253.192.191	Block	5
54.172.96.232	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 54.172.96.232	Block	4
54.172.96.232	United States	147.237.76.86	navy.idf.il	PHP Attempt	Block	3
109.64.148.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.114.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.114.160	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
109.64.148.230	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal/izkor/view_imgtop.asp	Block	2
98.139.14.250	United States	147.237.77.216	dover.idf.il	Double URL Encoding - parameter: utm_source=Copy+of+Weekly+Brief+%2FNovember+9%2C+2012&utm_campaign=Newsletter&utm_medium=email in www.idf.il/1283-17570-en/dover.aspx	Block	1
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	1
176.228.14.198	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$87 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.19.86.232	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$60 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/klali/null	Block	1
2.52.177.91	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58613&docid=65534	Block	1
80.246.138.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.181	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1235-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Unknown HTTP Request Method uA0[[#1]]TTA<K+Ã Ã eÃŠÃ%Ã?Ã%ÃŽÃ?i[[#22]]Ã?Ã,[[#17]]Ã.h in URL [[#2]]Ãæx@[[#31]]	Block	1
45.35.104.194		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/hebrew/main.asp	Block	1
98.139.14.251	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily_statistics/english/1.doc.	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?docid=64483	Block	1
79.180.114.186	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$106 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Illegal Byte Code Character in Header Name	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?&	Block	1
109.64.171.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
82.102.249.27	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.78.11	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 66.249.78.11	Block	1
172.82.175.253		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp>hebrew 	Block	1
157.55.39.139	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
104.247.216.236		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	1
185.89.217.231		147.237.77.74	law.idf.il	URL is Above Root Directory www.law.idf.il/./images/trans.gif	Block	1
79.181.228.172	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Illegal HTTP Version	Block	1
2.54.176.239	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
216.218.206.66	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
109.65.208.97	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58604&docid=67717	Block	1
84.108.168.122	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
176.13.0.134	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Illegal Byte Code Character in Method	Block	1