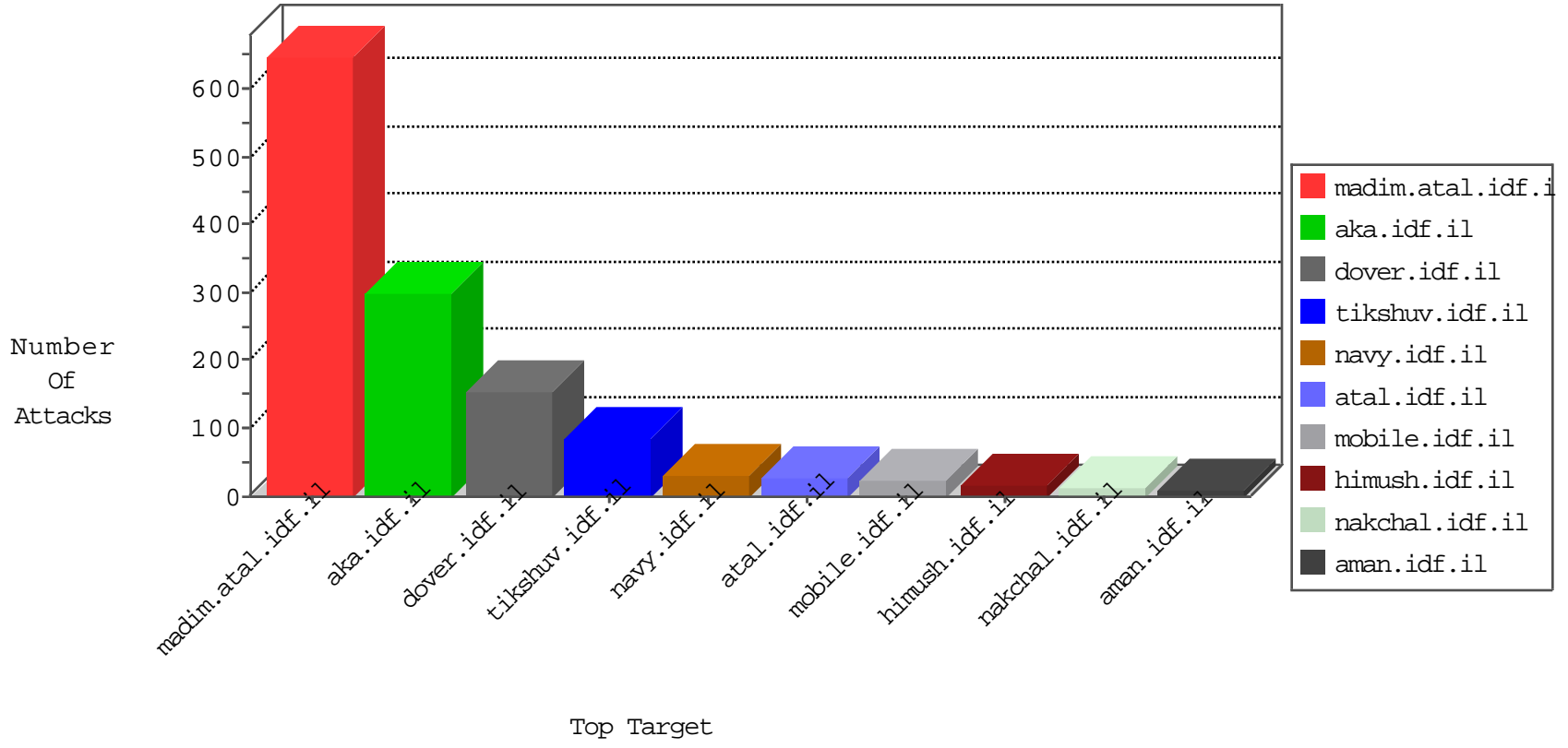


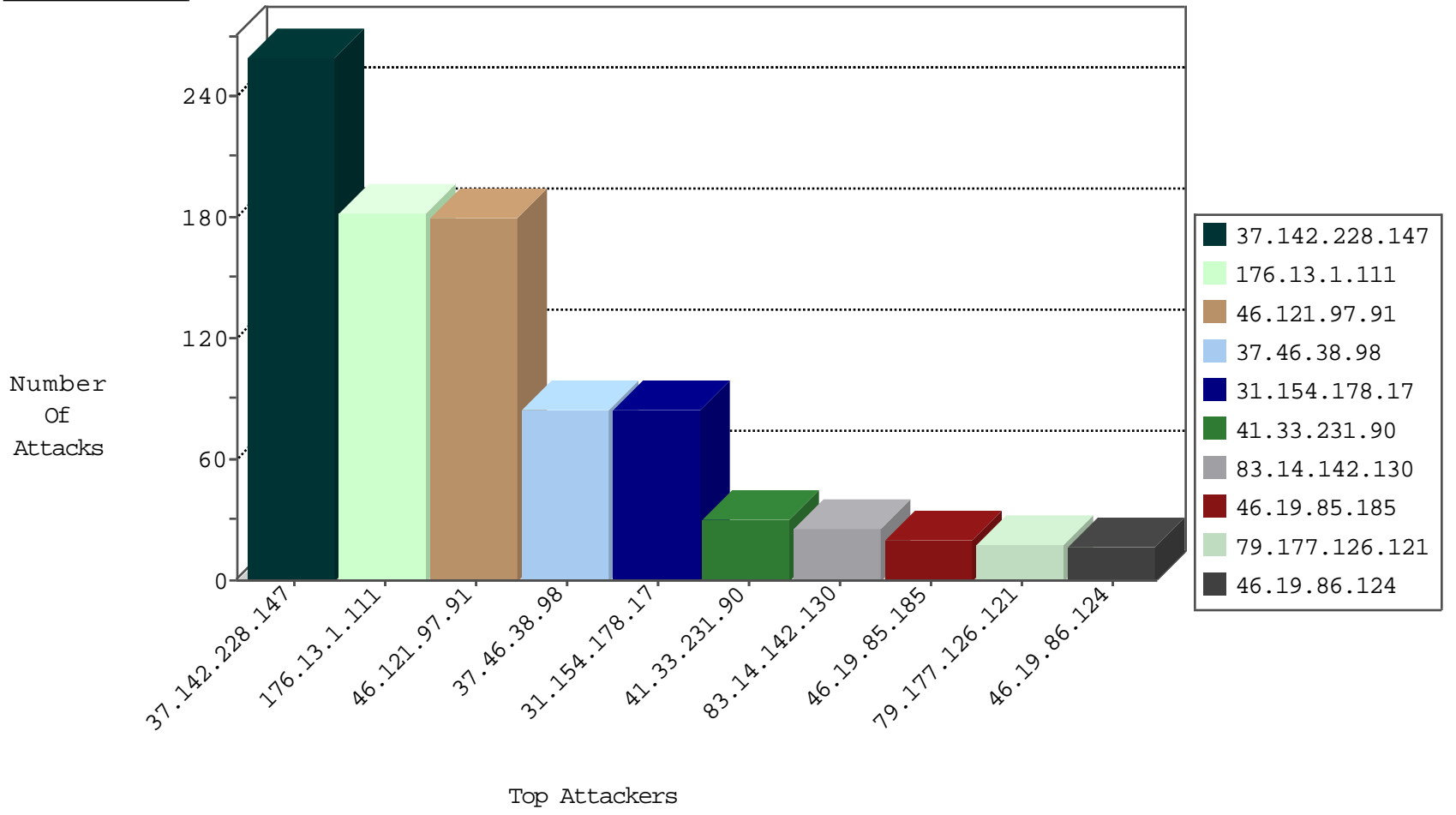
# IDF Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
105.200.64.238	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
185.130.5.224		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

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
66.249.69.122	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sA (2)	2
209.126.116.147	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
125.212.232.144	147.237.77.216	Vietnam	dover.idf.il	ET SCAN NMAP -sS window 2048	1
93.189.26.18	147.237.76.34	Austria	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
223.4.174.30	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
223.4.174.30	147.237.0.17	China	m.ny-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
125.212.232.144	147.237.77.216	Vietnam	dover.idf.il	ET SCAN NMAP -f -sS	1
79.181.61.112	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.10.155.230	147.237.77.74	Bulgaria	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
223.4.174.30	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.154.178.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.86.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
212.76.127.44	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
149.78.246.171	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.185	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.177.126.121	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.65.34.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.249.24	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.31.167	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.152.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
83.225.130.249	Italy	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
78.243.187.119	France	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
83.225.130.249	Italy	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.178.51	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
54.172.96.232	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
201.220.244.247	Chile	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.123	Israel	147.237.72.166	aka.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
64.246.187.42	United States	147.237.76.86	navy.idf.il	Header Rejection	header rejection pattern found in request	monitor	4
95.86.75.57	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
172.91.164.31		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.177.126.121	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
201.220.244.247	Chile	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.180.181.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.179.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.130.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.12		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.149.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.185	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.110.109.98	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.27.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.140.69	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
89.138.165.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.179.192	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
84.108.249.24	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
37.46.38.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
62.90.131.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.135.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.50.6	Russian Federation	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.14		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.97	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
37.142.228.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	142
37.142.228.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
176.13.1.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	100
46.121.97.91	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.121.97.91	Block	87
176.13.1.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
37.46.38.98	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 37.46.38.98	Block	82
46.121.97.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
46.121.97.91	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.121.97.91	Block	25
2.54.179.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	4
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	4
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	3
109.66.3.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	3
46.19.85.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	3
77.127.221.144	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	2
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	2
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	2
46.19.86.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	2
83.14.142.130	Poland	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
201.220.244.247	Chile	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 201.220.244.247 (Open Mode)	None	1
103.231.219.194	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
84.228.17.129	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/	Block	1
41.82.0.80	Senegal	147.237.76.86	navy.idf.il	E-mail collector robots 14	Block	1
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/pratim/pirteychayal	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Illegal Byte Code Character in Method	Block	1
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
2.54.187.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
139.18.44.158	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.78.94	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
41.82.0.80	Senegal	147.237.77.233	atal.idf.il	eMail Hoarding	Block	1
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/tizmoret	None	1
87.202.21.79	Greece	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	1
83.14.142.130	Poland	147.237.77.216	dover.idf.il	NULL Character in Method [[#11]]Y[[#0]]Ã-Ãž1Ã@Ã.Ã•ÃœÃ-ÃžÃ~iÃ?Ã†XÃ+:-[[#15]]IM[[#28]]/?ÃµÃ~Ã?Ã+Ã,:ÃžÃ«A	Block	1
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Abnormally Long Header Line request header name	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
46.121.97.91	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
201.220.244.247	Chile	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
85.75.57.102	Greece	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
41.82.0.80	Senegal	147.237.76.86	navy.idf.il	eMail Hoarding	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=60800	Block	1
5.175.13.138	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
149.78.246.171	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
45.55.131.62		147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/894-he/nakhal.aspxshared/usercontrols/headerupper/	Block	1
95.86.75.57	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/maslulimlist.aspx	Block	1