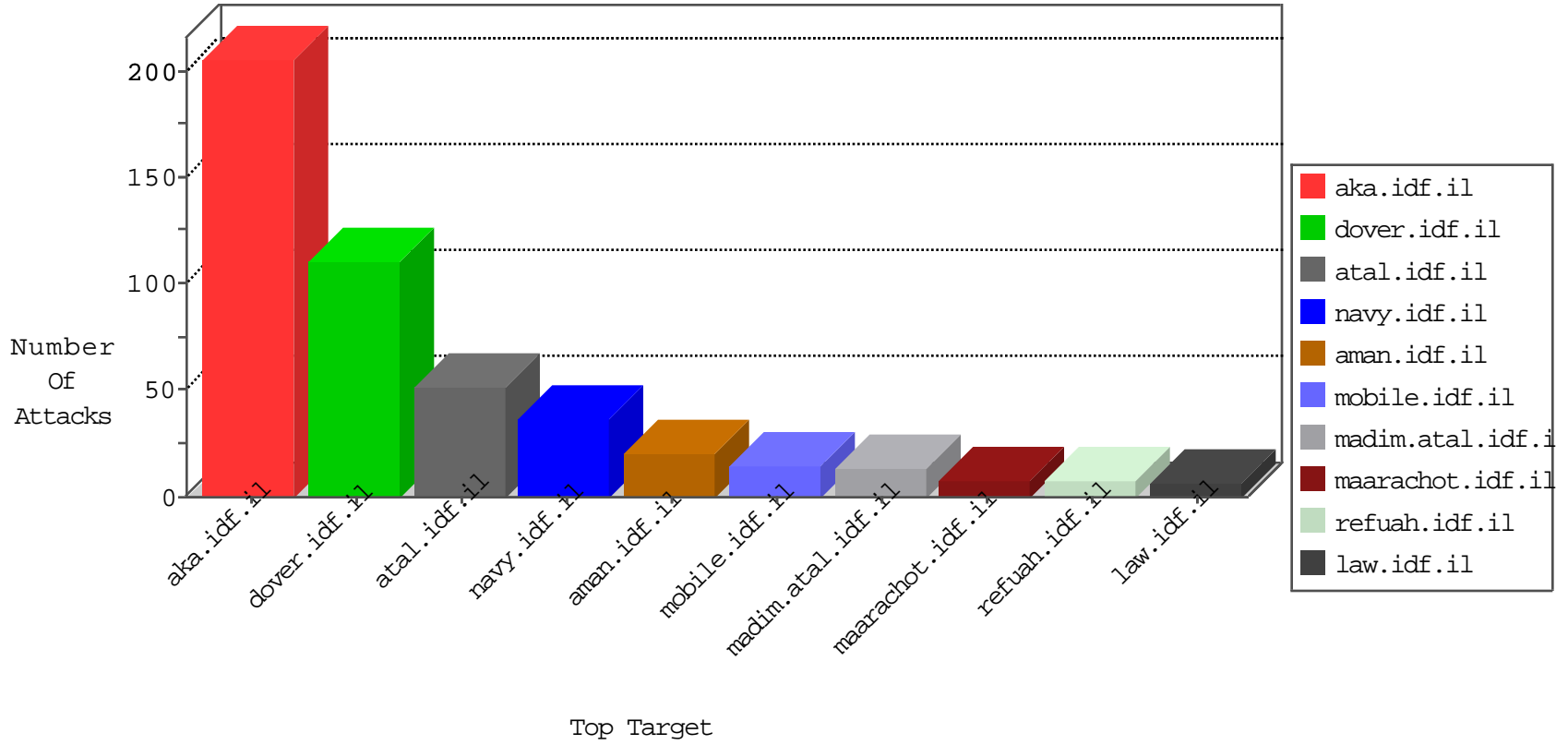


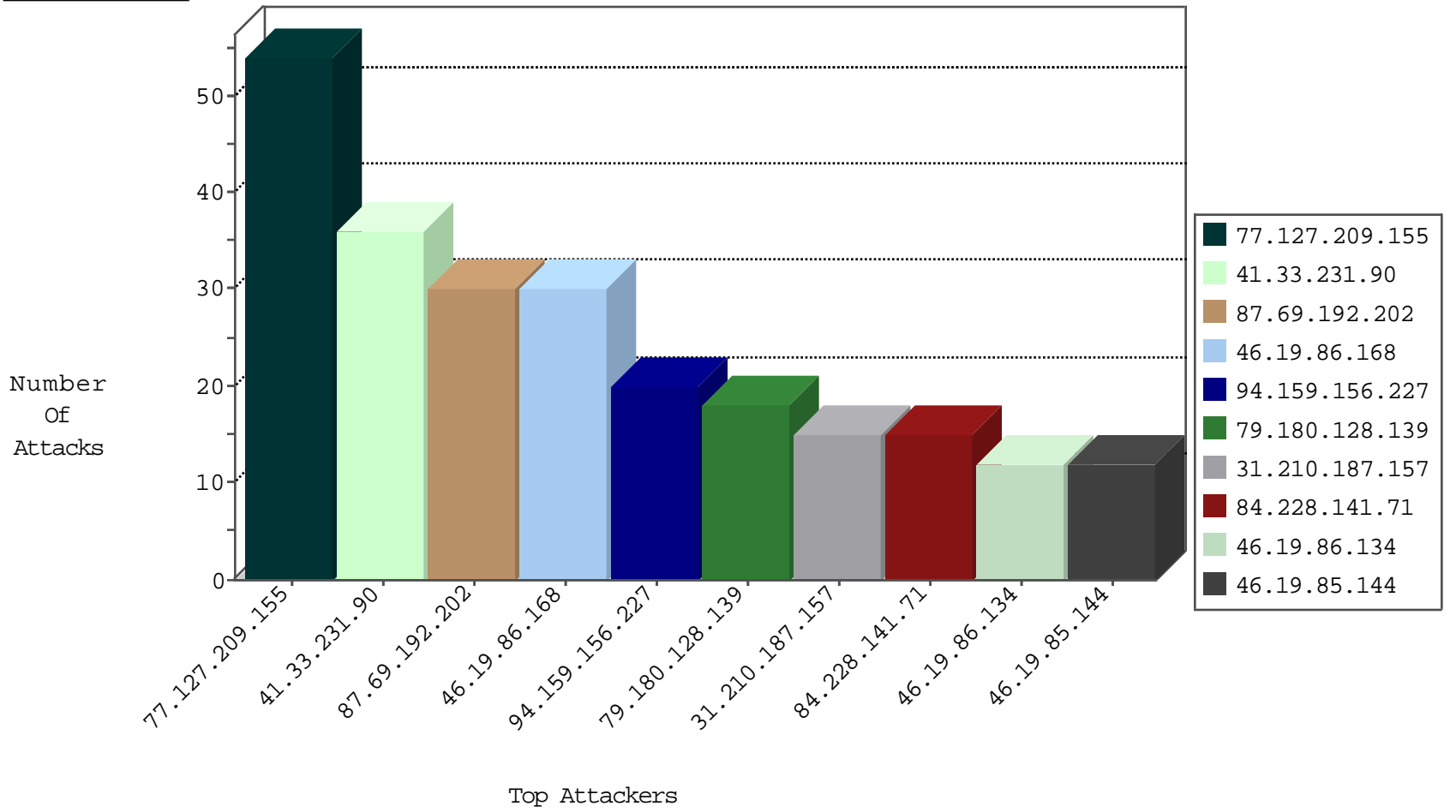
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
185.130.5.179		147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
201.92.187.72	Brazil	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.179		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.123	Italy	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
155.94.254.143	United States	147.237.76.147	chinuch.aka.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1

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	5
62.219.147.171	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
222.186.56.42	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.42	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.42	147.237.0.17	China	m.ny-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
95.156.251.10	147.237.0.19	Germany	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.42	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.42	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.77.234	Turkey	halag.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
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
87.69.192.202	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
46.19.86.168	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
94.159.156.227	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
84.228.141.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.134	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
31.210.187.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
8.37.237.232	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.86.168	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
80.246.139.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.210.187.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.128.139	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	6
109.66.3.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.131.54	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
185.3.144.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.230.86.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.180.128.139	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.64.120.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.103.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.125.74.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.128.139	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.177.34.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.150.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.38	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
213.57.74.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.235.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.128.139	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.65.178.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.172.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.141.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.177.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.94.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.78.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.139.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.195.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.134.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.128.139	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
31.210.186.144	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.188.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
154.118.111.55		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
31.210.186.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

02-12-2016-19:04:05 to 02-12-2016-20:04:05

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.142.64.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.253.136.164	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.20.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
216.72.40.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.176.133	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	2
37.26.149.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.190.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.5.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.114.179.211	Romania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
79.180.207.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.3	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/size338x0/sip_storage	Block	1
212.235.8.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/reserve	Block	1
84.110.80.130	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-12321-en	Block	1
185.32.236.97	Luxembourg	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
93.114.179.211	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
81.218.134.195	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	1
157.55.39.66	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
84.110.80.130	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
37.142.172.153	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.172.153	Block	1
185.32.236.97	Luxembourg	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
94.159.156.227	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
82.117.245.43	Ukraine	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/404.aspx'	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/rankfs.html	Block	1
157.55.39.228	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/giyus/kiosk/general.aspx	Block	1
87.69.192.202	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1440-he/atal.aspx	Block	1
77.125.119.68	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
41.228.47.61	Tunisia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
198.161.119.4	Canada	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.97.154.204	Romania	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.69.32	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2418.jpg	Block	1
87.69.192.202	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
77.125.119.68	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
41.228.47.61	Tunisia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
207.46.13.41	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
109.97.154.204	Romania	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
84.110.35.63	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.34	Block	1