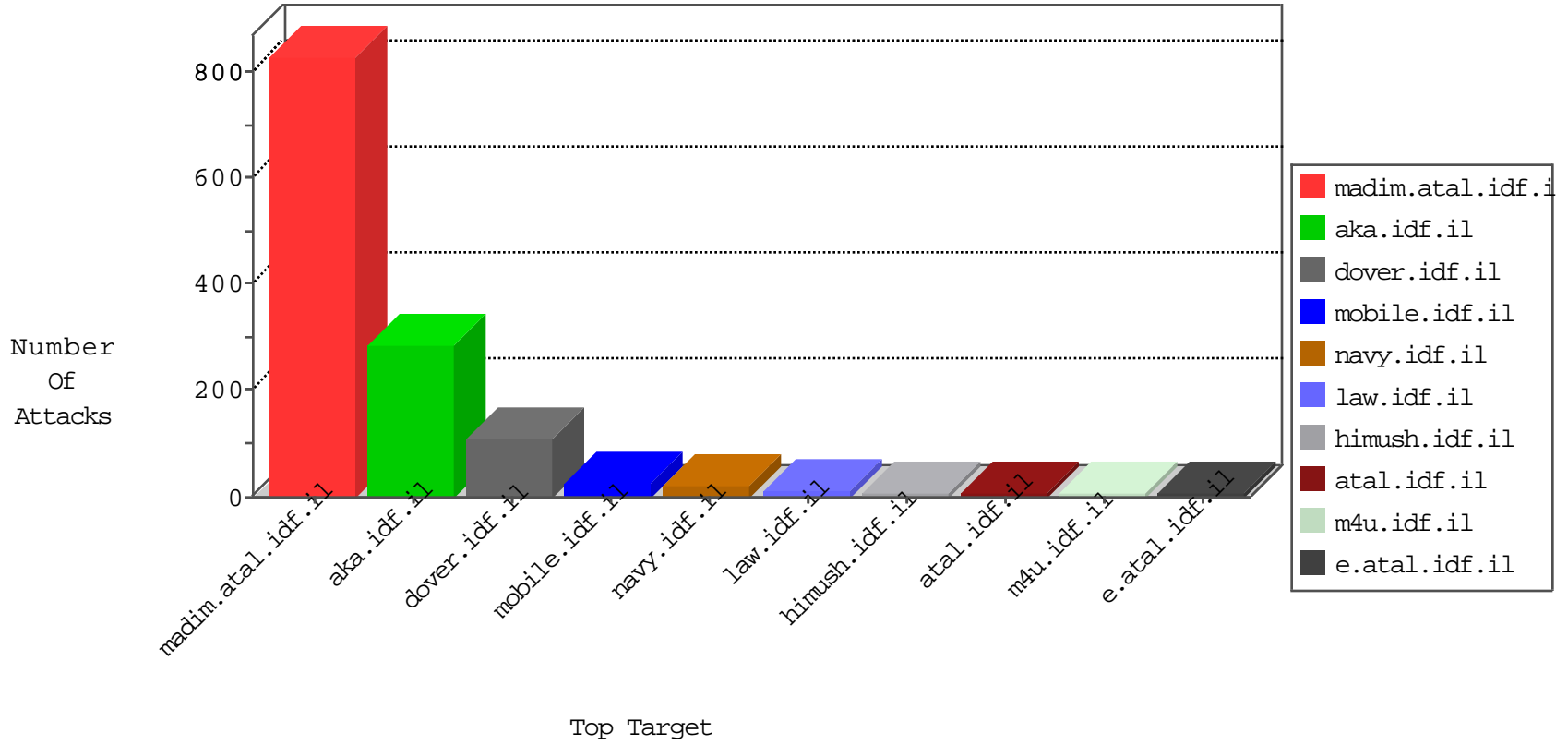


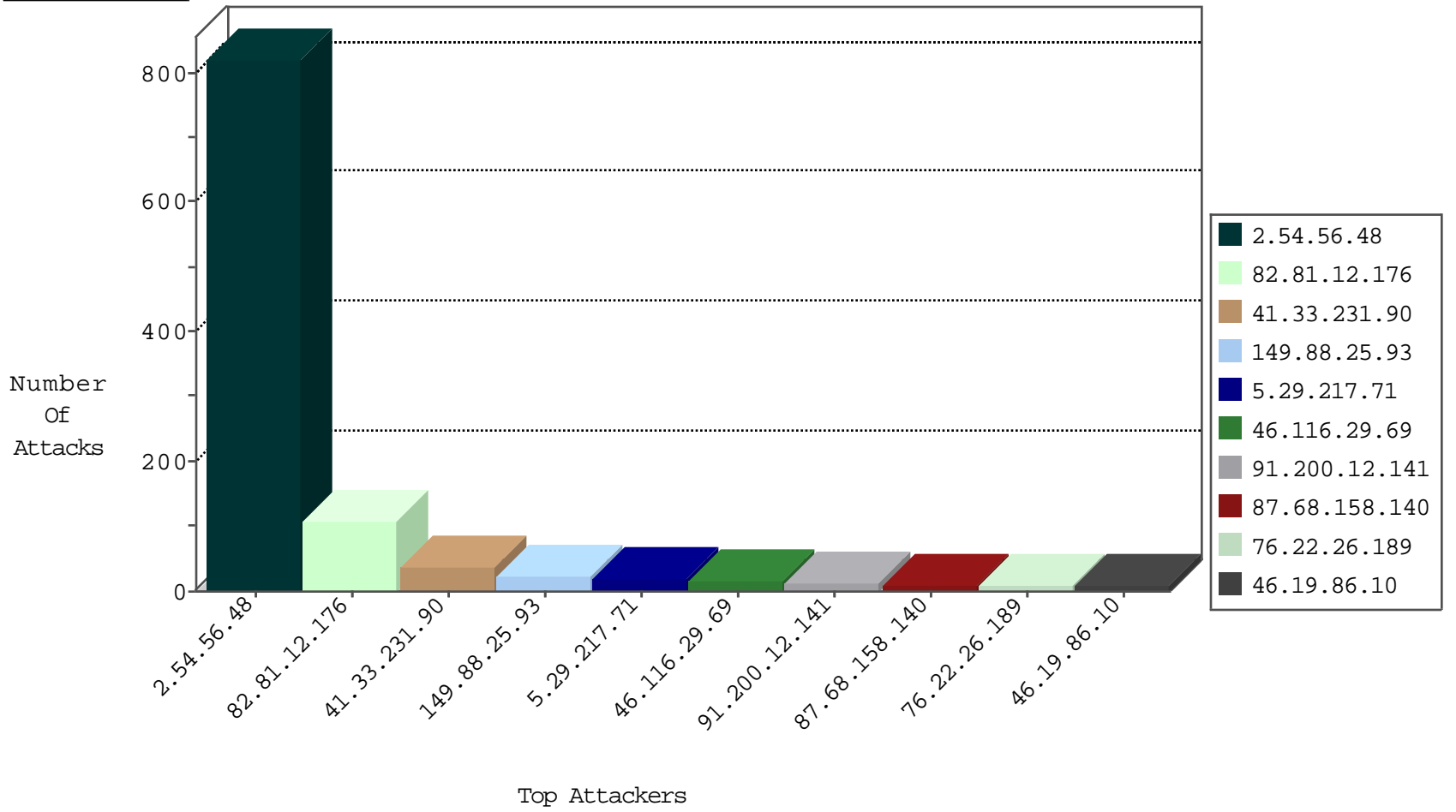
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	108
101.141.10.131	Japan	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	4
185.130.5.224		147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
66.240.219.146	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

01-30-2016-08:04:04 to 01-30-2016-09:04:04

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	3
61.182.170.38	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
61.182.170.38	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.182.170.38	147.237.76.176	China	test.noore.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 3072	1
218.246.0.97	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
13.75.42.200	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
210.93.50.130	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
195.154.214.162	147.237.76.34	France	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
61.182.170.38	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.182.170.38	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 4096	1
218.246.0.97	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.77.233	Turkey	atal.idf.il	ET SCAN NMAP -sS window 1024	1
210.93.50.130	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
198.20.69.74	147.237.76.147	United States	chinuch.aka.idf.il	ET DROP Dshield Block Listed Source	1
195.154.214.162	147.237.8.28	France	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.8.24	United States	e.lifestyle.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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
149.88.25.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
94.159.147.76	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
76.22.26.189	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
77.127.152.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.158.140	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.135.106	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.175.19	Israel	147.237.77.243	mobile.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
203.143.188.11	India	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
37.247.36.68	Netherlands	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
91.200.12.141	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	5
5.29.217.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	5
46.116.29.69	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.29.217.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.187.158	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
5.102.254.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.7	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
46.116.29.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
77.125.1.101	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
94.230.86.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.125.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
176.13.14.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.217.71	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.64.7.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.165.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.13.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.1.101	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
109.67.252.218	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.217.71	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
79.183.114.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.50.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.217.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
87.68.158.140	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.65.125.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
66.249.78.199	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.116.29.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.3.144.89	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
149.88.206.108	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.10	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.7.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.46.39.66	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.57.169.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.56.48	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.56.48	Block	527
2.54.56.48	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.56.48	Block	187
2.54.56.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
37.26.147.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
87.68.85.250	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/popups/markivsachar.aspx parameter	None	4
109.253.147.110	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	3
89.139.229.106	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	2
84.108.7.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
141.212.122.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
50.63.196.103	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp/wp-admin/	Block	1
79.179.9.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
67.19.79.218	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to /robots.txt	Block	1
173.252.88.187	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.1.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.111.38.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
191.232.136.173	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
74.208.16.113	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp-admin/	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
149.78.34.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.242.228.108	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.180.35.88	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 79.180.35.88	Block	1
219.94.128.34	Japan	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/test/wp-admin/	Block	1
67.19.79.218	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to /robots.txt	Block	1
176.13.14.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.186.48.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.117.22.137	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
2.52.17.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.73.149	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/mas.aspx	Block	1
192.116.1.192	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
78.25.123.255	Russian Federation	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
149.78.204.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.210.187.158	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$employmentStatusDay in aka.idf.il/main/sachar/payslips.aspx	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
80.179.9.139	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	1
178.154.189.204	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
46.117.22.137	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$emailUpdate\$rptEmailSubjectsLi in www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	None	1
2.54.32.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
203.33.121.38	Australia	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/old/wp-admin/	Block	1
78.25.123.255	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.78.147	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/kapatz/default.aspx	Block	1
149.88.25.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il./	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
80.179.96.90	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
185.120.125.32		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
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakchal.idf.il/1073-he/nakchal.aspx	Block	1