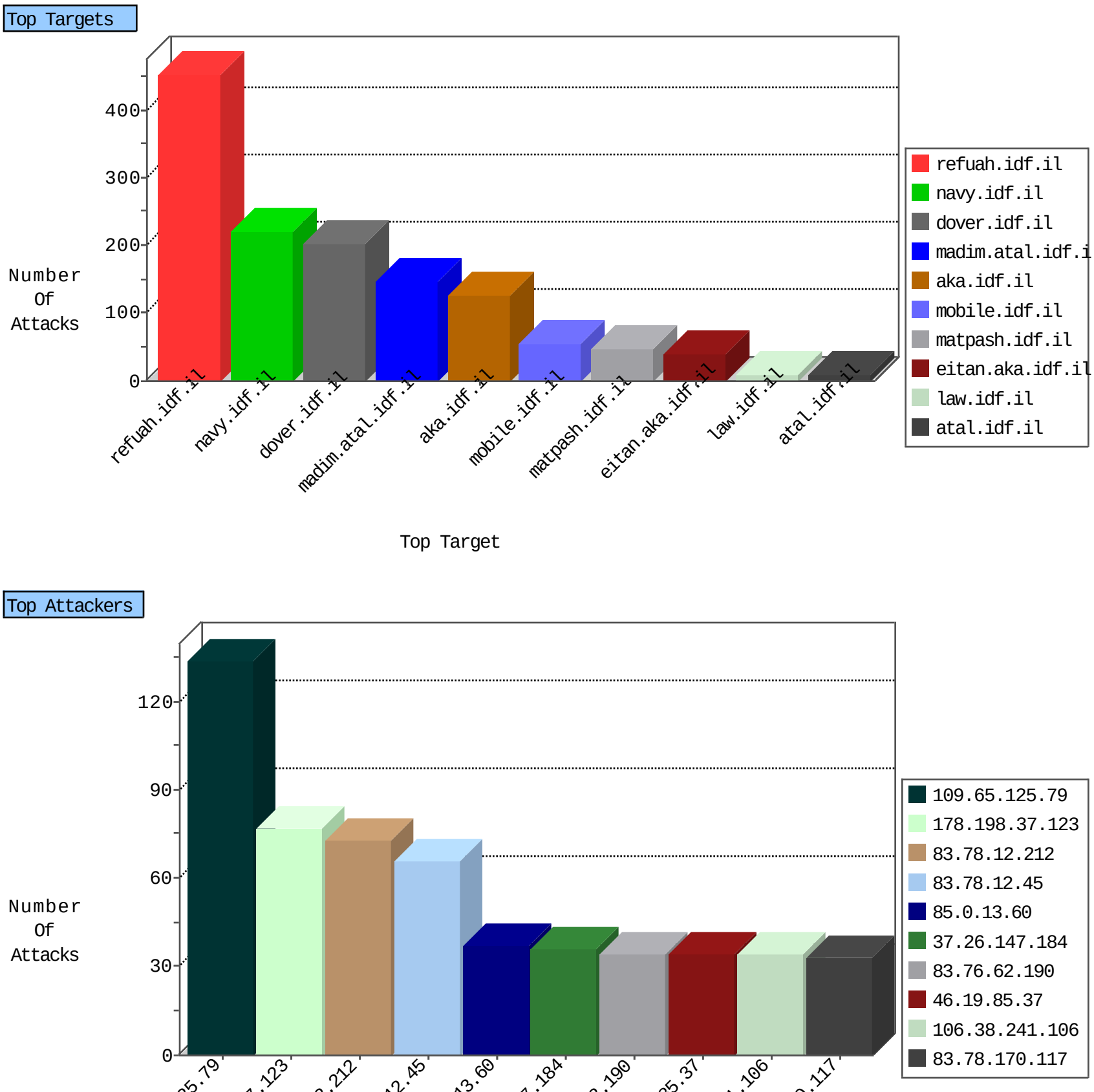
10-02-2016-16:04:08 to 10-02-2016-17:04:08

IDF Under Attack Daily Report



10-02-2016-16:04:08 to 10-02-2016-17:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.233	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
134.147.203.115	Germany	147.237.76.31	nakchal.idf.il	Black List	drop	6
37.26.149.163	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

10-02-2016-16:04:08 to 10-02-2016-17:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	34
91.121.86.136	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
91.121.86.136	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.129	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-02-2016-16:04:08 to 10-02-2016-17:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.70	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
192.198.151.44	147.237.72.167	Europe	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
168.63.52.221	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.229.172.116	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
168.63.52.221	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
221.229.172.116	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
168.63.52.221	147.237.0.33	United States	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.223.76.249	147.237.76.30	Bolivia	himush.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
163.172.129.15	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
168.63.52.221	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
168.63.52.221	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.86.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.63.52.221	147.237.77.170	United States	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.255.90.133	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
168.63.52.221	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
168.63.52.221	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
168.63.52.221	147.237.72.217	United States	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.229.172.116	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
168.63.52.221	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.36.35.241	147.237.76.148	Russian Federation	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
168.63.52.221	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.0.33	United Kingdom	idf.il	ET SCAN NMAP -sS window 1024	1
168.63.52.221	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.76.106	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
168.63.52.221	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
14.152.59.11	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
168.63.52.221	147.237.77.121	United States	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.53.142.171	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
168.63.52.221	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

10-02-2016-16:04:08 to 10-02-2016-17:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
109.65.105.178	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.63	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
83.78.12.212	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	15
83.78.12.212	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	15
83.78.12.45	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
83.78.12.212	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	15
83.78.12.45	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	14
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	14
83.78.12.212	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	14
77.125.60.197	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
83.78.12.212	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	14
85.65.87.177	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
83.78.12.45	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	13
46.19.85.37	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
79.177.219.39	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
83.78.12.45	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
83.78.12.45	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	12
109.253.133.126	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.37	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
85.64.71.250	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
46.19.85.211	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
37.26.147.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
83.78.170.117	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	8
46.19.85.211	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
85.0.13.60	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
85.0.13.60	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
83.76.62.190	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	8
213.57.87.62	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	8
85.0.13.60	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	8
46.19.86.196	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.0.13.60	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	7
83.76.62.190	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
83.78.170.117	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	7
46.19.86.193	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
178.199.204.38	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	7
83.78.170.117	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
77.138.174.165	France	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
83.76.62.190	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	7
46.19.85.39	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
83.76.62.190	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.65.87.177	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
85.0.13.60	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
178.199.204.38	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.178	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

10-02-2016-16:04:08 to 10-02-2016-17:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.125.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	134
77.139.20.102	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	4
31.154.45.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.127.23.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
83.53.250.36	Spain	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.idf.il/1038-en/dover.aspx	Block	2
46.133.119.60	Ukraine	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
208.81.64.248	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.i	Multiple Abnormally Long Request from 169.229.3.91	Block	1
2.53.162.43	Israel	147.237.76.86	navy.idf.il	Distributed Cookie Tampering on token: __atrfs	None	1
79.179.21.239	Israel	147.237.76.86	navy.idf.il	Distributed Cookie Tampering on token: __atrfs	None	1
66.249.64.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1248-he/atal.aspx	Block	1
46.19.86.118	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
77.127.245.147	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.102.6.30	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.i	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
2.53.183.57	Israel	147.237.76.86	navy.idf.il	Distributed Cookie Tampering on token: __atrfs	None	1
66.249.69.116	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/25112010maskorot.aspx	Block	1
46.19.86.118	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
109.253.130.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.21.11	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
84.111.94.35	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
66.249.75.167	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
46.19.86.118	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	NULL Character in Method =ã'5Â[[#28]]ØÊÆOjz…EÔ!“”ùäyÏŠÁDì[[#0]]Î“F(Ñö\seð[[#11]]o•8‘¶[[#14]]{ qÃu(¬• #012MËE‰	Block	1
141.226.217.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.64.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1232-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in Header Name	Block	1
37.26.147.217	Israel	147.237.76.86	navy.idf.il	Suspicious Response Code	Block	1
87.69.3.182	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
77.126.18.29	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
46.19.86.118	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvs=57f1133c05d54fbc000; _pk_ref.20.8afc=%5B%22%22%2C%22%22%2C1475416896%2C%22https%3A%2F%2Fwww.google.co.il%2F%22%5D; _pk_id.20.8afc=737ac48827dc740a.1475416895.1.1475416896.1475416895.; _pk_ses.20.8afc=*	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
157.55.39.254	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
79.177.219.39	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.58	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	147.237.0.19	madim.atal.idf.il	Malformed URL	Block	1
46.19.85.39	Israel	147.237.76.86	navy.idf.il	Cookie Tampering on cookie __atrfs: Expected ab/	None	1
94.43.75.93	Georgia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1

10-02-2016-16:04:08 to 10-02-2016-17:04:08