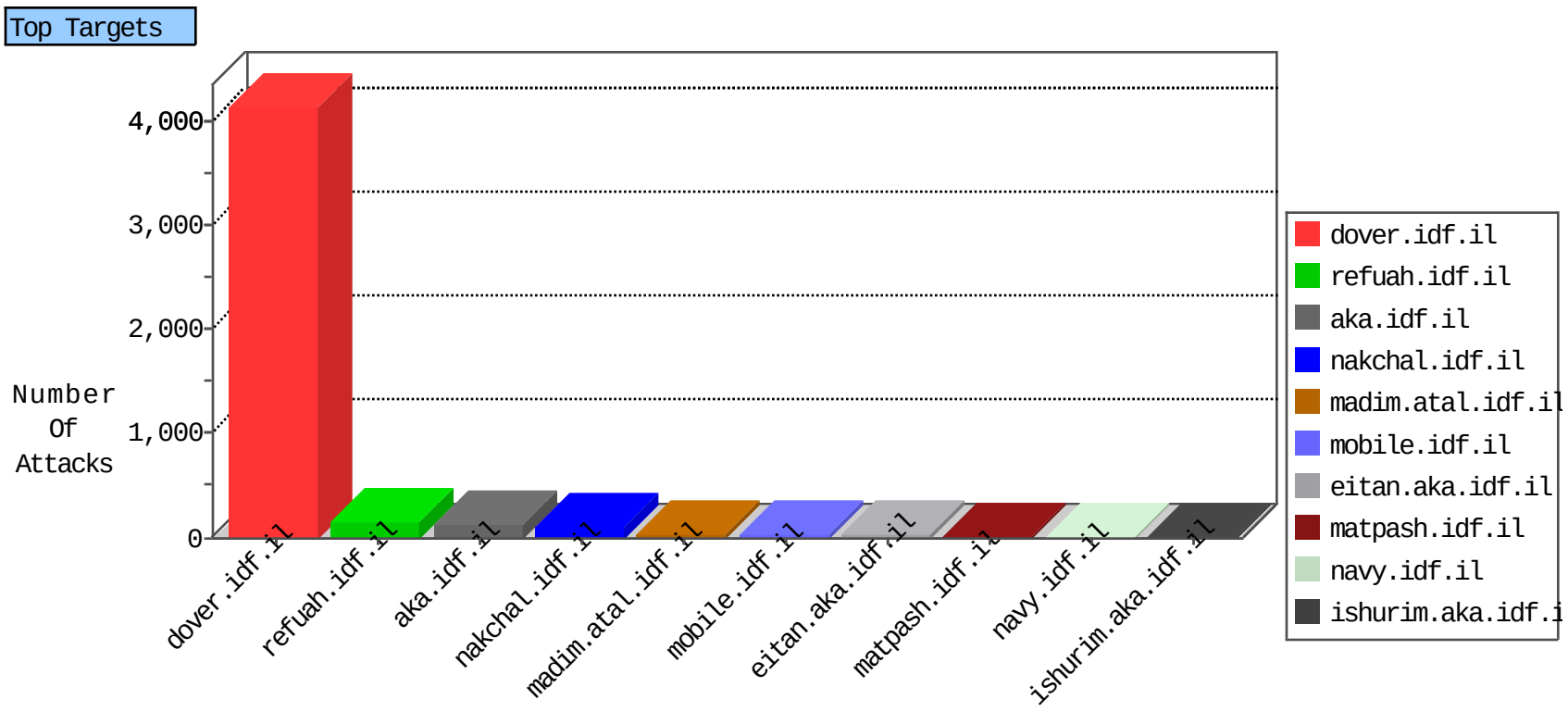
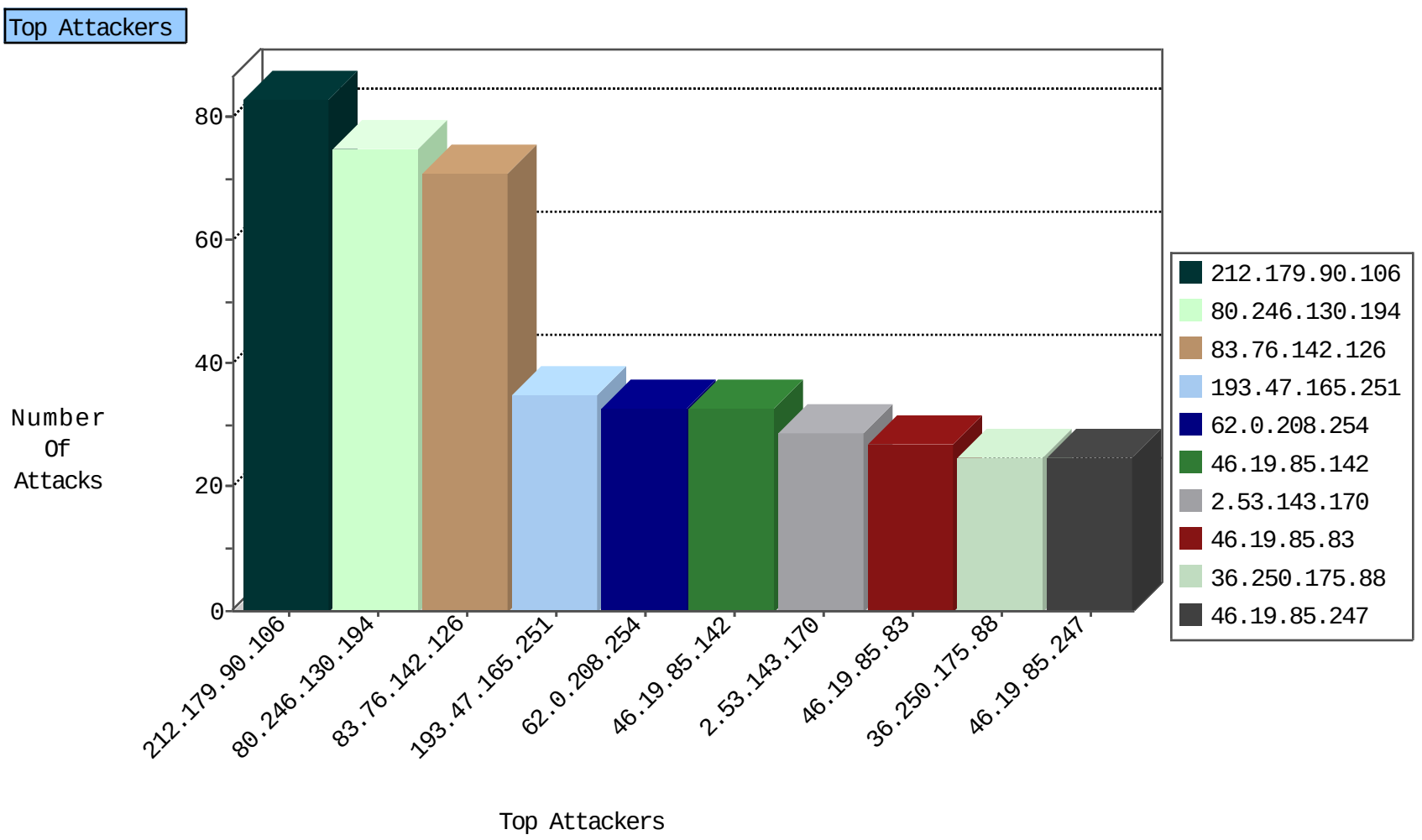
09-28-2016-14:04:09 to 09-28-2016-15:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-28-2016-14:04:09 to 09-28-2016-15:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.149.93	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
69.30.193.254	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
69.30.227.221	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
173.208.198.10	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
93.174.94.235	Netherlands	147.237.76.202	e.halag.idf.il	Black List	drop	1
43.239.221.49	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
198.204.255.76	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
142.54.180.69	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
52.28.32.164	Germany	147.237.76.196	e.sviva.idf.il	JLM_Purple_Con_Limit_Https	drop	1
198.204.255.77	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
69.30.227.220	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
173.208.150.116	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
52.28.32.164	Germany	147.237.76.201	e.atal.idf.il	JLM_Purple_Con_Limit_Https	drop	1
63.141.231.212	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1

09-28-2016-14:04:09 to 09-28-2016-15:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.43.128.9	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
71.13.87.122	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-28-2016-14:04:09 to 09-28-2016-15:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.208.165.101	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
176.228.54.22	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
115.47.12.162	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
109.64.111.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.3.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.144.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
46.19.86.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.255.99.142	147.237.72.166	Argentina	aka.idf.il	portscan: TCP Distributed Portscan	1
2.55.161.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.114.177.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.211.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.86.120.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.189.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.106	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1
220.231.195.122	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.86.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -f -sS	1
46.19.85.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-28-2016-14:04:09 to 09-28-2016-15:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
80.246.130.194	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	74
193.47.165.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
62.0.208.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	33
2.53.143.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
46.19.85.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.85.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
5.102.229.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
176.13.232.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
109.253.145.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
176.228.33.78	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
83.76.142.126	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
46.19.85.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
83.76.142.126	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	15
213.151.35.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.253.139.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
185.137.19.92		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.253.147.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.142	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
83.76.142.126	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	14
62.219.148.215	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
83.76.142.126	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	13
83.76.142.126	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
23.79.224.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
185.103.12.66	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
176.13.240.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
2.53.141.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
176.13.7.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.55.151.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
80.178.201.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
2.55.182.77	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.8.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
194.90.232.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.116.142.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
91.135.102.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.142	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
89.237.114.236	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10

09-28-2016-14:04:09 to 09-28-2016-15:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
36.250.175.88	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 36.250.175.88	Block	16
2.53.149.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
185.32.179.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
36.250.175.88	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	5
46.19.86.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.13.243.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
66.249.69.85	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter lang in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
212.34.23.135	Jordan	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
45.33.137.185	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2016/lobby.aspx	Block	1
85.250.149.60	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
2.55.19.147	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.57.253.198	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.76.109	Israel	147.237.72.166	aka.idf.il	Unknown Parameter D.. in www.aka.idf.il/giyus/general/	None	1
194.90.147.229	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	1
46.19.86.243	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
36.250.175.88	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
109.67.115.210	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
81.218.168.149	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.69.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8802-he/refuah.aspx	Block	1
176.228.33.78	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method POST for www.eitan.aka.idf.il/1105-he/contactus.aspx	None	1
46.19.85.83	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
87.70.18.251	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
2.55.153.79	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.228.44	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter PageNum in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
54.210.231.197	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/web-console/serverinfo.jsp	Block	1
207.46.13.176	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/...	Block	1
37.26.147.145	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
130.193.37.2	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/favicon.ico	Block	1
84.94.159.254	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1756	Block	1
185.32.179.159	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.156	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
93.172.58.159	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus9	Block	1
5.255.253.34	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
77.139.171.63	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/kamlar/klali/default.asp	Block	1
66.249.64.160	Israel	147.237.77.74	law.idf.il	Illegal URL Path Encoding www.law.idf.il/templates/getfile/getfile.aspx?filenamem	Block	1
212.34.23.135	Jordan	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
37.26.148.197	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
132.66.223.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.108.32.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$emailUpdate$rptEmailSubjectsList$ctl02$cbEmailSubject in www.aka.idf.il/main/giyus/faq.aspx	None	1
2.53.32.34	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.76.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/שקופית2	Block	1
46.19.85.156	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method late in URL	Block	1
95.86.82.166	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
79.181.13.48	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
212.34.23.135	Jordan	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1

09-28-2016-14:04:09 to 09-28-2016-15:04:09