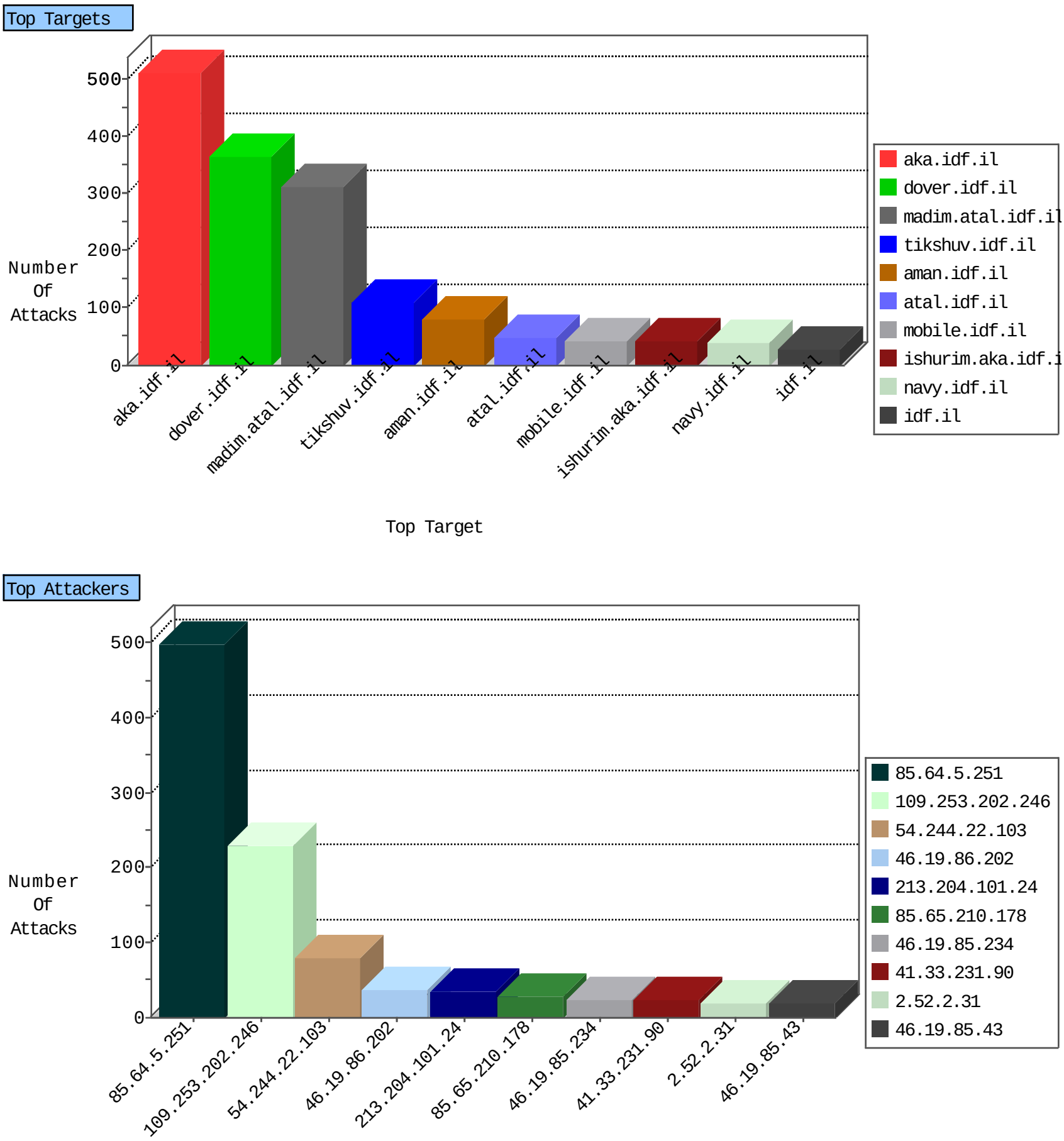
02-04-2016-13:04:04 to 02-04-2016-14:04:04

IDF Under Attack
Daily Report



02-04-2016-13:04:04 to 02-04-2016-14:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.5.251	Israel	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	3262
85.64.5.251	Israel	147.237.0.33	idf.il	TCP Scan (vertical)	drop	1945
85.64.5.251	Israel	147.237.72.156	aman.idf.il	TCP Scan (vertical)	drop	1940
85.64.5.251	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	8
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
198.199.127.149	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
123.195.224.211	Taiwan	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
159.122.252.41	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
54.67.38.74	United States	147.237.0.15	kosher-kravi.idf.il	DOS-httpdx-hreadrequest-FS	dest-reset	1
198.199.127.149	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
54.67.38.74	United States	147.237.76.30	himush.idf.il	DOS-httpdx-hreadrequest-FS	dest-reset	1

02-04-2016-13:04:04 to 02-04-2016-14:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.5.251	Israel	147.237.72.166	aka.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	9
85.64.5.251	Israel	147.237.72.166	aka.idf.il	2809: HTTP: IIS TRACK Method	Block	9
106.38.241.106	China	147.237.77.216	dover.idf.i	C103: HTTP: User Agent Sogou+web+spider	Block	1
85.64.5.251	Israel	147.237.72.166	aka.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1

02-04-2016-13:04:04 to 02-04-2016-14:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
85.64.5.251	147.237.72.166	Israel	aka.idf.il	SERVER-WEBAPP TRACE attempt	19
85.64.5.251	147.237.72.166	Israel	aka.idf.il	GPL WEB_SERVER TRACE attempt	16
85.64.5.251	147.237.72.166	Israel	aka.idf.il	SERVER-WEBAPP WEB-INF access	4
37.142.148.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.5.251	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.157.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.5.251	147.237.0.33	Israel	idf.il	ET SCAN Potential VNC Scan 5800-5820	1
2.54.31.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.88.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.80.155.224	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
79.183.117.237	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.93.7	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sA (2)	1
162.222.185.165	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.174	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	1
85.64.5.251	147.237.77.216	Israel	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.85.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.84	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.46.35.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.5.251	147.237.0.33	Israel	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.54.134.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.5.251	147.237.0.33	Israel	idf.il	ET SCAN NMAP -sS window 1024	1
212.179.221.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.116.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
79.181.32.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
162.222.185.165	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
66.249.81.201	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1
85.250.31.243	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.75.214	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
85.64.5.251	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.146	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-04-2016-13:04:04 to 02-04-2016-14:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	70
213.204.101.24	Lebanon	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
2.52.2.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
212.219.249.99	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
82.80.86.129	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
104.131.40.139	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.138.78	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
169.254.187.219		147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	10
37.26.149.248	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.65.210.178	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	9
85.65.210.178	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.173.144.3	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.129.19	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.152.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
212.179.214.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.200.180	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.36.206	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
130.203.136.75	United States	147.237.77.74	law.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	6
176.13.5.79	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.125.27		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.179.214.29	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.65.60.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.130.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.6.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
132.76.10.42	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.234	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.179.214.29	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
37.26.148.182	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.5.174	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
31.210.187.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
80.240.78.234	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
85.65.210.178	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
85.64.5.251	Israel	147.237.0.33	idf.il	drop		drop	4
46.19.85.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
81.218.200.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.181.22	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
77.125.4.197	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
85.65.210.178	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3

02-04-2016-13:04:04 to 02-04-2016-14:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.5.251	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.64.5.251	Block	156
109.253.202.246	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.202.246	Block	115
109.253.202.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	115
46.19.86.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37
85.64.5.251	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.64.5.251	Block	29
46.19.85.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
46.19.85.234	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.234	Block	17
37.142.68.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
85.64.5.251	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 85.64.5.251	Block	9
80.246.136.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
85.64.5.251	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	6
85.64.5.251	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	6
85.64.5.251	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	6
85.64.5.251	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	4
104.131.40.139	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 104.131.40.139	Block	4
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	3
109.253.134.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.116.164.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.64.5.251	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 85.64.5.251	Block	2
80.246.137.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.151.41.140	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.151.41.140	Block	2
79.182.29.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	2
85.64.5.251	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1824-he/dover.aspx	Block	2
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	2
213.57.158.224	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$20 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_ref.20.8afc=["","",1454586211,"http://m.facebook.com"];	Block	1
85.64.5.251	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucNewsFlashControl$datepicker in www.idf.il/1153-he/dover.aspx	Block	1
85.64.5.251	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1779-he/dover.aspx	Block	1
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	1
85.64.5.251	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1841-he/dover.aspx	Block	1
85.65.200.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$emailUpdate$txtEmail in www.aka.idf.il/main/giyus/faq.aspx	None	1
85.64.5.251	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
46.19.85.21	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
85.64.5.251	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1815-he/dover.aspx	Block	1
85.64.5.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter -s in www.aka.idf.il/main	None	1
84.228.185.60	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.228.185.60	Block	1
176.13.5.79	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.64.5.251	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1381-he/dover.aspx	Block	1
85.64.5.251	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1785-he/dover.aspx	Block	1
79.181.217.210	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl67 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.253.129.19	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
85.64.5.251	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method tssc=facebook%3B7; in URL	Block	1
85.64.5.251	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucNewsFlashControl$datepicker in www.idf.il/1841-he/dover.aspx	Block	1
85.64.5.251	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1780-he/dover.aspx	Block	1
85.64.5.251	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube	Block	1
85.64.5.251	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1133-he/dover.aspx	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
124.123.21.71	India	147.237.77.216	dover.idf.il	PHP Attempt	Block	1

02-04-2016-13:04:04 to 02-04-2016-14:04:04