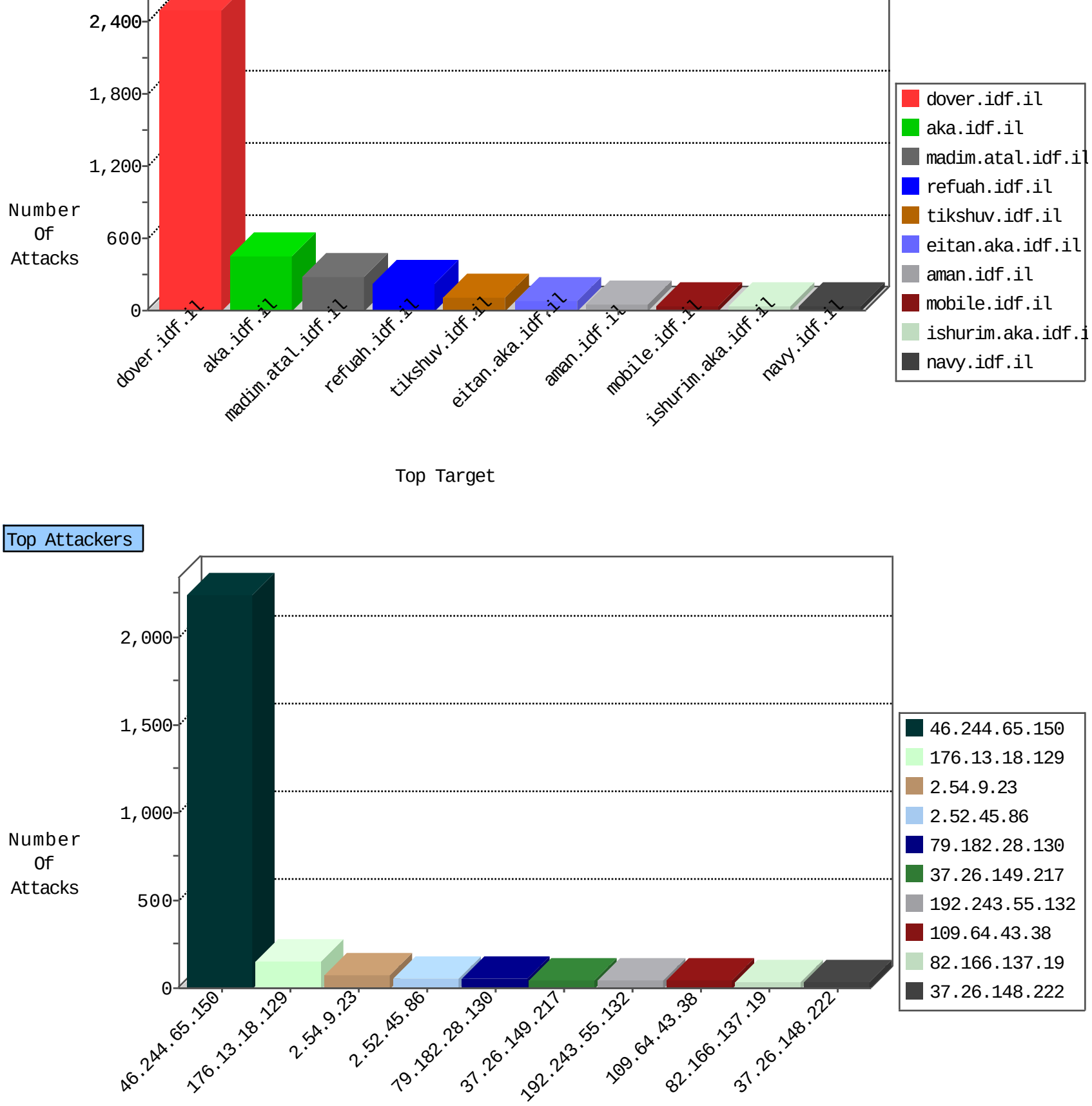
03-03-2016-10:04:03 to 03-03-2016-11:04:03

IDF Under Attack Daily Report



03-03-2016-10:04:03 to 03-03-2016-11:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.244.65.150	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2246
82.166.137.19	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	292
79.176.134.51	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
79.176.134.51	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
82.145.217.34	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
203.185.34.216	Hong Kong	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	2
203.185.34.216	Hong Kong	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	2
184.105.139.102	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
24.237.158.16	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.110	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
203.185.34.216	Hong Kong	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
104.245.97.224		147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
203.185.34.216	Hong Kong	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
176.13.18.129	Israel	147.237.0.19	madim.atal.idf.il	DOSS-SSL-ClearText	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
82.145.221.157	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1

03-03-2016-10:04:03 to 03-03-2016-11:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.228.30.3	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
192.118.12.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
37.26.146.251	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
2.54.140.235	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.253.134.43	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.85.24	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-03-2016-10:04:03 to 03-03-2016-11:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.183.55.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.160.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.46.16	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.220.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.57.81	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.109.199.190	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.200.122	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.200.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.132.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.74.103.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.105	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
46.19.85.81	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.125.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.236.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
207.232.18.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.253.134.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-03-2016-10:04:03 to 03-03-2016-11:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.182.28.130	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
109.64.43.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
66.249.93.121	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	27
2.54.9.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	26
2.52.45.86	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
66.249.93.125	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	24
37.26.148.222	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	21
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	19
2.54.13.125	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
2.52.172.135	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
31.154.27.186	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
80.246.130.211	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
109.64.231.186	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	17
2.54.9.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
2.54.9.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	15
2.54.9.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
104.131.214.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
37.26.148.222	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
5.22.135.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.37.124	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.34.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
109.186.148.199	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.102.9.3	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
94.230.93.153	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
46.116.56.18	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
94.230.93.195	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
109.253.137.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.45.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.45.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.177.33.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.184.13	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.2.204	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.45.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
2.54.167.208	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.45.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.117.175.118	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.23.95	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.234.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.200.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.155.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.10.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.45.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
94.230.93.147	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
81.218.55.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

03-03-2016-10:04:03 to 03-03-2016-11:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	145
37.26.149.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
85.64.56.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
62.0.25.121	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 62.0.25.121	Block	15
2.54.7.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
80.246.139.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
46.19.86.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
37.26.149.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.130.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
37.26.149.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 82.80.196.44	Block	6
66.249.66.76	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
109.186.148.199	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
185.32.179.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.219.83	Israel	147.237.76.30	himush.idf.il	Multiple Unauthorized URL Access from 109.253.219.83	Block	3
2.54.37.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.131.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.186.148.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.149.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
104.131.214.94	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 104.131.214.94	Block	3
2.52.164.12	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.86.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.94.15.145	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.94.15.145	Block	2
109.253.222.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.2.204	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Email in mobile.idf.il/sachar/createaccount	Block	2
66.220.145.243	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr	Block	1
94.230.93.156	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.charts.js	Block	1
84.111.200.183	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl17 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.85.9	Israel	147.237.76.42	refuah.idf.il	Distributed Abnormally Long Request	Block	1
94.230.93.249	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery.nyromodal-1.6.2.js	Block	1
2.54.56.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
94.230.93.214	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
94.230.93.179	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/giyus/general.aspx	Block	1
157.55.39.58	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/library/manage/resource/getfilecontent.hh.asp	Block	1
104.131.214.94	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1132-8613-he/navy.aspx.aspx	Block	1
94.230.93.140	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/images/shared/mailthis.gif	Block	1
194.90.178.37	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1240-he/atal.aspx	Block	1
94.230.93.233	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/scroller/jquery.jcarousel.css	Block	1
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.178.186.11	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.18.129	Israel	147.237.0.19	madim.atal.idf.i	Cookie Tampering on cookie Login: Expected ********** ********** ********** *, Observed ********** ********** **********	None	1
94.230.93.198	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
94.230.93.163	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/3480.jpg	Block	1
66.249.64.74	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl41 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.85.9	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version __atuvs=56d7f4da5ee7e1a2000	Block	1
94.230.93.252	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/1.he/langstyle.css	Block	1
2.54.174.30	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1

03-03-2016-10:04:03 to 03-03-2016-11:04:03