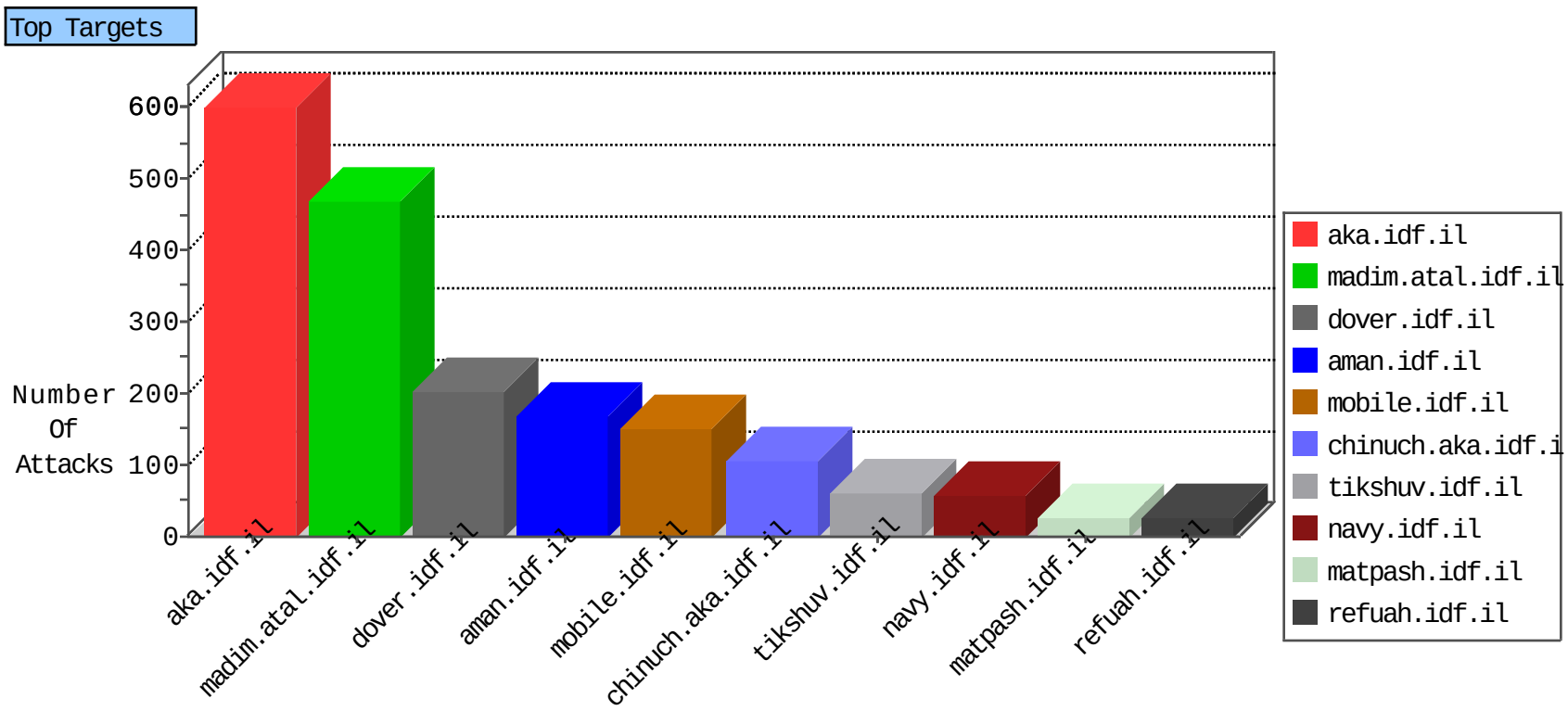
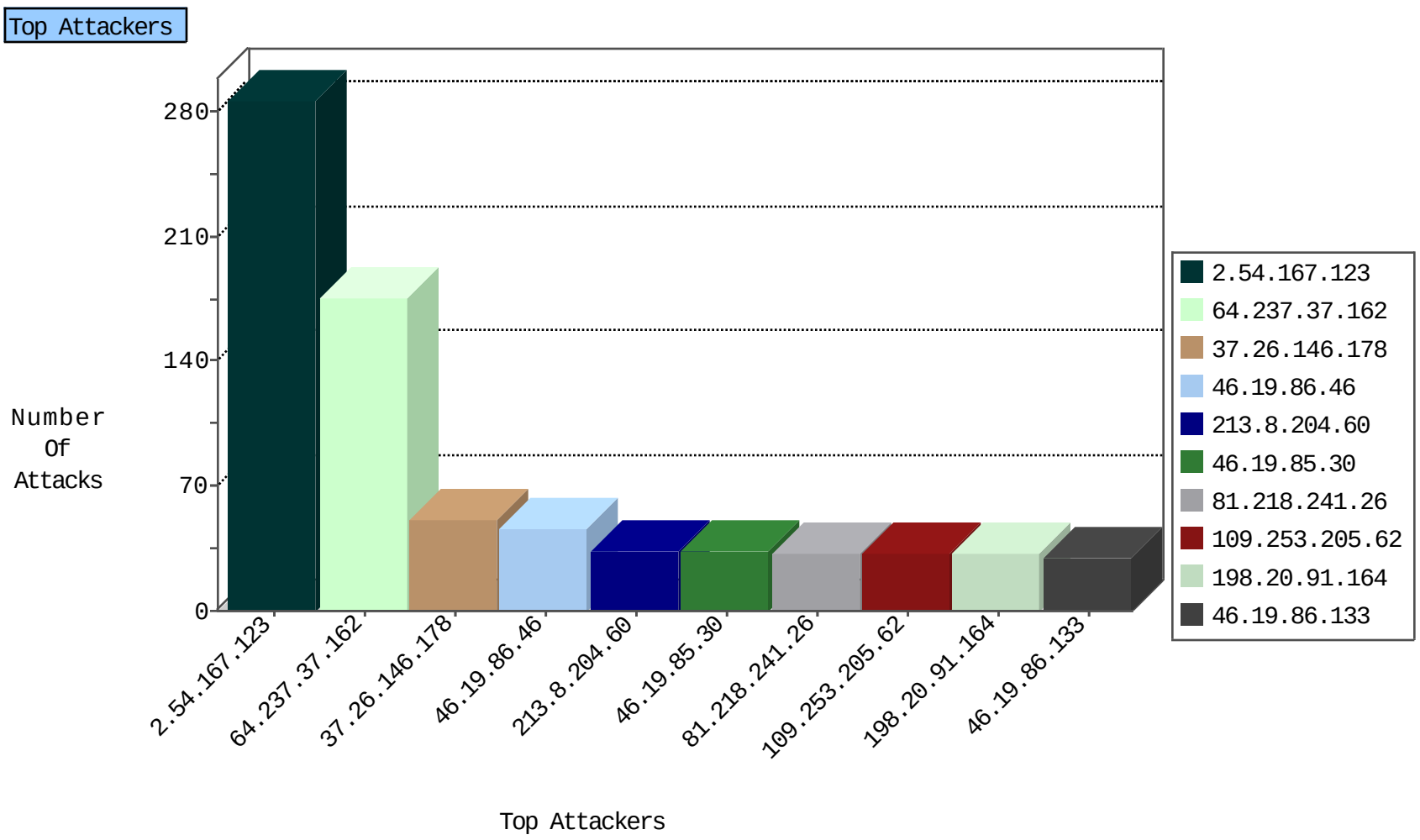
02-10-2016-16:04:08 to 02-10-2016-17:04:08

IDF Under Attack
Daily Report



Top Target



Top Attackers

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

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
213.8.204.60	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	27
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
109.253.222.170	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
109.65.58.177	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
159.220.78.114	India	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
74.91.28.59	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
159.220.78.115	India	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
74.91.28.61	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
142.54.169.162	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
159.220.78.116	India	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.220.78.113	India	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
208.110.85.58	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
155.94.254.143	United States	147.237.72.166	aka.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
198.20.69.74	United States	147.237.76.201	e.atal.idf.i	13840: TLS: OpenSSL Heartbeat Packet	Block	1

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

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
79.182.0.150	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.215.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.139.48	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.120	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN Potential SSH Scan	1
77.126.209.102	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.115.252.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
130.211.100.171	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.19.115.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.158.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.48.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.69.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.7.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
207.232.46.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.9.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.195.104	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.118.73.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.87.144.145	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
164.41.209.89	147.237.76.198	Brazil	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.30	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
129.171.150.150	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
5.28.177.107	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.194.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.190.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.102.169.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
64.237.37.162	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	88
64.237.37.162	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	88
79.179.195.97	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.85.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
46.19.86.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
46.19.86.46	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
198.20.91.164	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
198.20.91.164	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
82.166.0.86	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
192.118.78.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.26.147.203	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
212.179.21.194	Israel	147.237.76.202	e.halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
81.218.241.26	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.147.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.116.54.221	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.2.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.67.195.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.205.62	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
94.230.86.84	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.94	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
85.64.111.55	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	7
79.178.58.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.179.17.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.206.88	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.144.123	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.21.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
112.198.103.194	Philippines	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.12.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.2.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.56.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.27.105.104	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.21	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.126.1.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.90.216.42	Israel	147.237.72.166	aka.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
2.54.140.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.0	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.4.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.21	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.175.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5

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

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
77.125.158.83	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
94.230.86.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.167.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	155
2.54.167.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
37.26.146.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
46.19.86.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
109.253.156.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
2.54.167.123	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.167.123	Block	24
89.139.170.199	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	24
109.253.205.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.19.86.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
85.65.167.127	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 85.65.167.127	Block	12
188.143.232.26	Russian Federation	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 188.143.232.26	Block	8
46.19.86.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
188.143.232.26	Russian Federation	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 188.143.232.26	Block	6
37.26.147.203	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.13.12.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.46	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
50.63.197.202	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 50.63.197.202	Block	4
188.143.232.26	Russian Federation	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 188.143.232.26	Block	4
37.26.147.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.182.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.161.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.33.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
95.35.91.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.12.46	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
109.253.205.62	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.3.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.182.38.253	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Illegal Byte Code Character in URL	Block	2
188.143.232.26	Russian Federation	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 188.143.232.26	Block	2
37.26.149.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.2.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.182.38.253	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
128.232.110.28	United Kingdom	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
79.182.38.253	Israel	147.237.72.167	ishurim.aka.idf.i	Illegal Byte Code Character in Header Name	Block	1
94.159.177.181	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$7 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
78.58.67.148	Lithuania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
50.63.197.202	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
188.143.232.26	Russian Federation	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/931-he/	Block	1
82.166.0.86	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	1
79.182.38.253	Israel	147.237.72.167	ishurim.aka.idf.i	Multiple Abnormally Long Request from 79.182.38.253	Block	1
46.19.85.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.182.38.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
5.28.177.107	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$61 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.52.38.83	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
85.65.167.127	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
68.180.228.112	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/navmenu/	Block	1
207.46.13.152	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1560-en/dover.aspx"	Block	1
79.183.231.14	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1

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