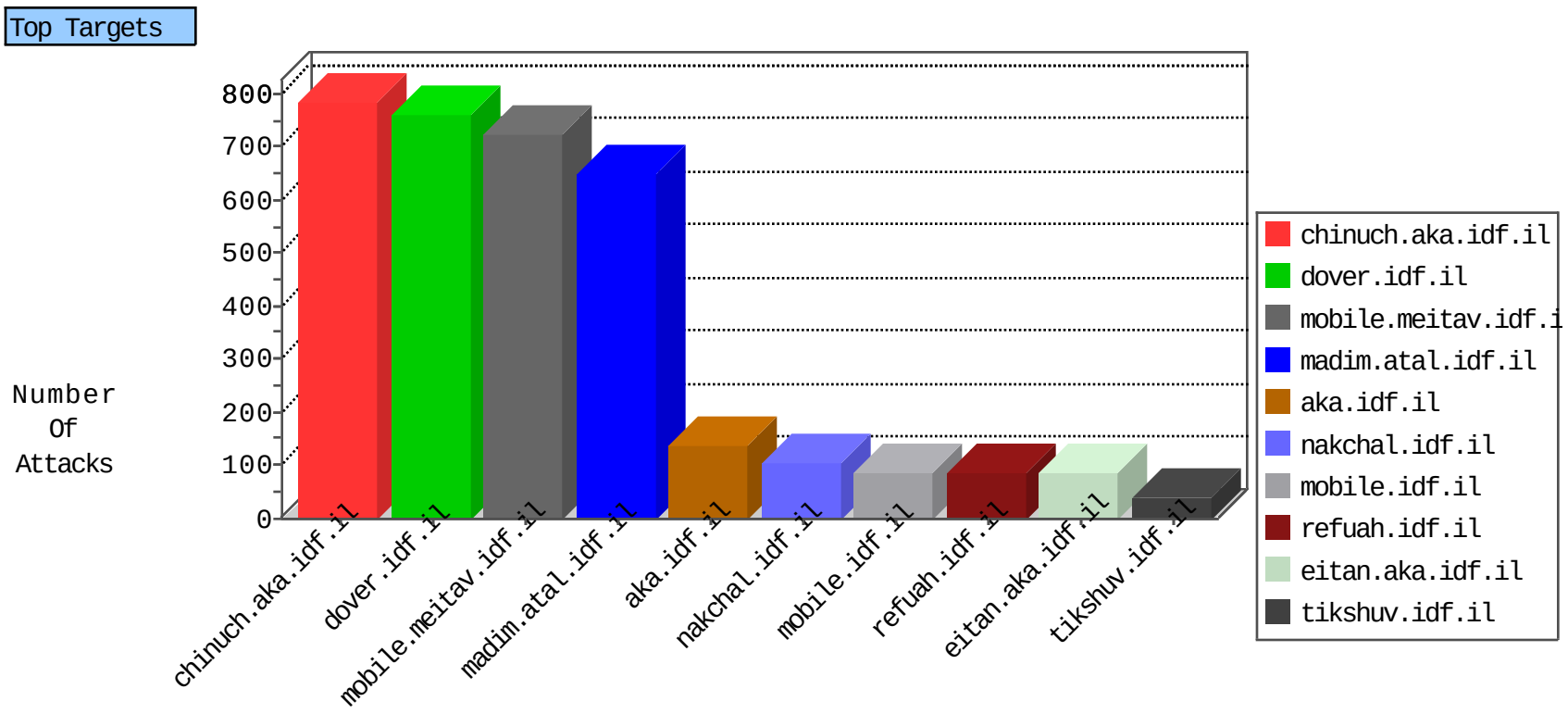
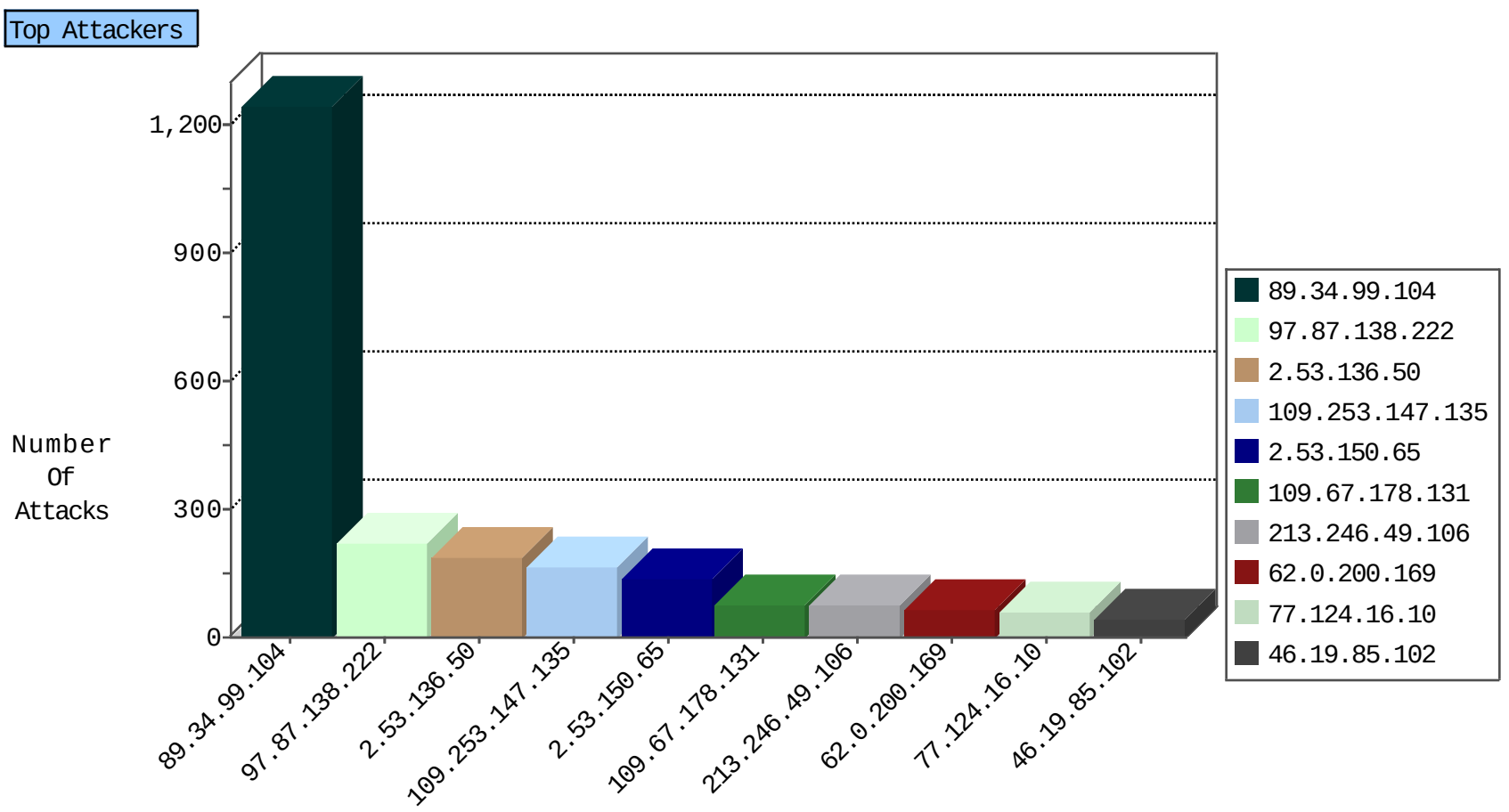
09-25-2016-09:04:06 to 09-25-2016-10:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-25-2016-09:04:06 to 09-25-2016-10:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.237.230	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
176.106.229.97	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.253.128.151	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
80.246.136.43	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
2.55.4.238	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.128.40.162	Switzerland	147.237.76.197	e.himush.idf.il	Black List	drop	1
5.102.195.1	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
109.253.219.15	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
191.96.249.37	Chile	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
45.32.26.222	Netherlands	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

09-25-2016-09:04:06 to 09-25-2016-10:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.246.49.106	France	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
202.124.242.10	Australia	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
49.236.200.182	Malaysia	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
213.246.49.106	France	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
213.246.49.106	France	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
74.208.154.12	United States	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
74.208.154.12	United States	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1
240.0.10.13		147.237.72.167	ishurim.aka.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1

09-25-2016-09:04:06 to 09-25-2016-10:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.246.49.106	147.237.76.31	France	nakchal.idf.il	SQL Injection - Select From	51
202.124.242.10	147.237.77.74	Australia	law.idf.il	SQL Injection - Select From	15
49.236.200.182	147.237.77.233	Malaysia	atal.idf.il	SQL Injection - Select From	14
74.208.154.12	147.237.76.31	United States	nakchal.idf.il	SQL Injection - Select From	8
218.205.151.198	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
59.46.193.114	147.237.72.167	China	ishurim.aka.idf.il	GPL SCAN nmap TCP	1
46.120.128.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.129.148.230	147.237.77.235	Latvia	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.26.222	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
185.129.148.230	147.237.77.179	Latvia	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.216	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
128.139.23.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.54.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.38.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.152.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.205.151.198	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
212.199.104.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.44.103	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.130.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.32.26.222	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1
185.129.148.230	147.237.77.234	Latvia	halag.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.26.222	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1
176.13.9.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.128.147	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.121.221.160	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1

09-25-2016-09:04:06 to 09-25-2016-10:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.34.99.104	Romania	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	640
89.34.99.104	Romania	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	606
97.87.138.222	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	116
97.87.138.222	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	105
109.67.178.131	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	76
109.65.97.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
62.0.200.169	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	34
62.0.200.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
46.19.86.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
62.0.222.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
46.19.85.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
213.41.149.222	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
46.19.85.102	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.22	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
46.19.85.22	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.85.102	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
62.219.161.88	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
109.253.219.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.146.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.6.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
2.55.133.174	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
109.253.204.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
77.125.40.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.21.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
82.166.200.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.159	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
84.111.28.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.196.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.181.123.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
141.226.232.16	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.116.177.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.181.205.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.13.11.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.27.105.134	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.117.38.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
155.254.239.91	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
37.26.146.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.66.96.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.234.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.129.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
147.236.32.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

09-25-2016-09:04:06 to 09-25-2016-10:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.147.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	162
2.53.136.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	136
2.53.150.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	133
77.124.16.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
2.53.136.50	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	53
46.19.85.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
176.13.19.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
2.55.57.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
2.55.187.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
80.246.138.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
132.64.158.150	Israel	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 132.64.158.150	Block	4
91.227.165.5	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
91.227.164.5	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
87.68.5.162	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	3
46.19.86.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
91.227.165.5	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 91.227.165.5	Block	3
2.53.174.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.90.85.210	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$ContentPlaceHolder1$FAQListViewTemplate1$InternalSearch1$txtFreeTextSearch in www.law.idf.il/338-he/patzar.aspx	Block	3
132.64.158.150	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	3
91.227.164.5	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 91.227.164.5	Block	2
46.19.86.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
194.9.252.237	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 194.9.252.237	Block	2
80.246.140.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	2
185.32.179.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.81.88.212	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method fied-Since: in URL sun,	Block	1
82.81.94.10	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.181.101	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
217.194.198.30	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
176.13.236.7	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2306.jpg	Block	1
109.66.184.21	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.27	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.139.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.26	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
91.227.164.5	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
82.81.109.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.190.110	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
217.194.198.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.32.179.26	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8763-he/refuah.aspx	Block	1
109.67.225.161	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
87.69.235.119	Israel	147.237.0.19	madim.atal.idf.il	Multiple Unauthorized URL Access from 87.69.235.119	Block	1
194.9.252.237	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/portalmiluim/templates/home.asp	Block	1
66.249.64.118	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/apple-app-site-association	Block	1
132.64.158.150	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/894-he/tizmoret	Block	1
46.19.86.27	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
76.206.13.139	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1

09-25-2016-09:04:06 to 09-25-2016-10:04:06