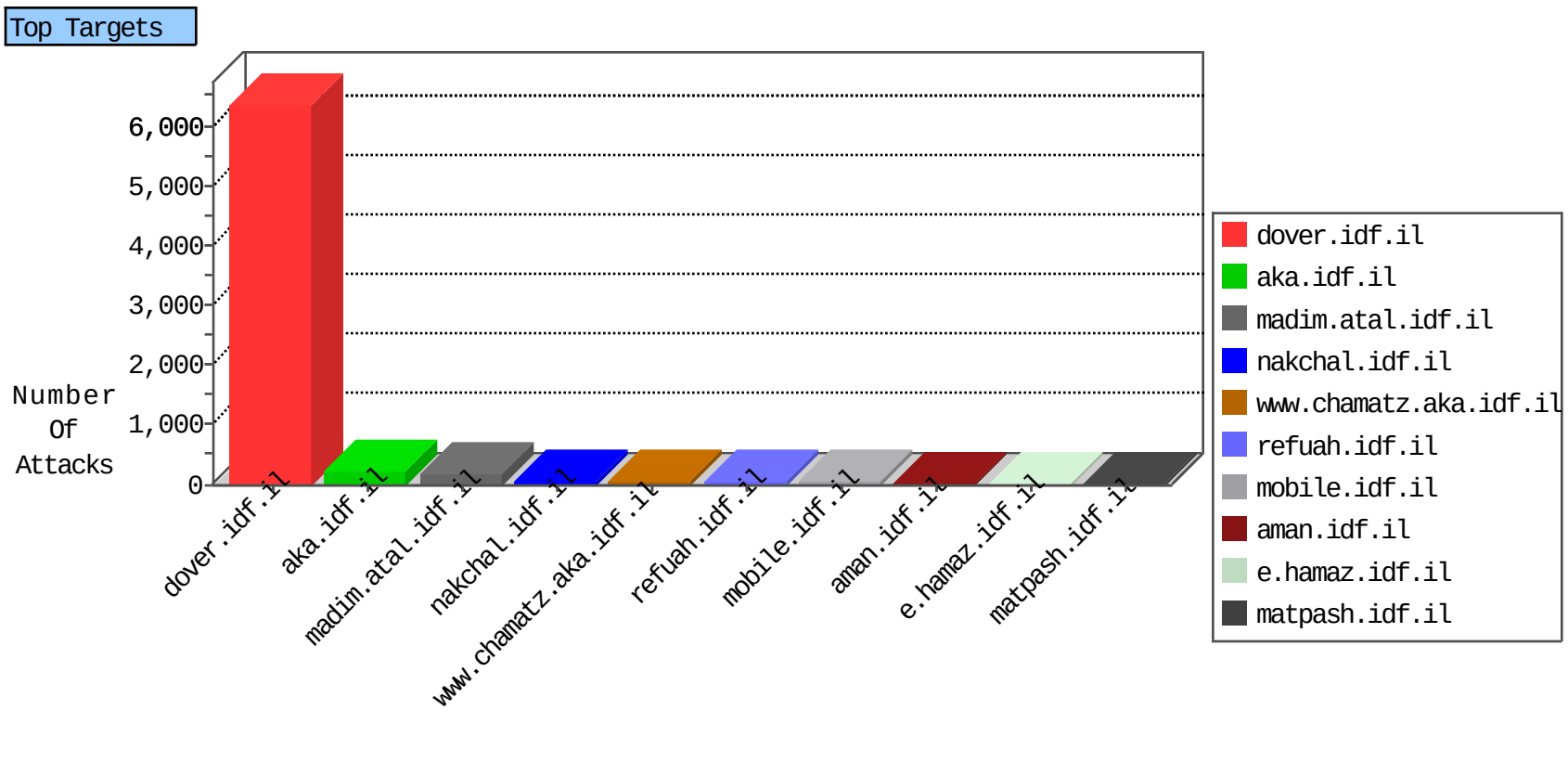
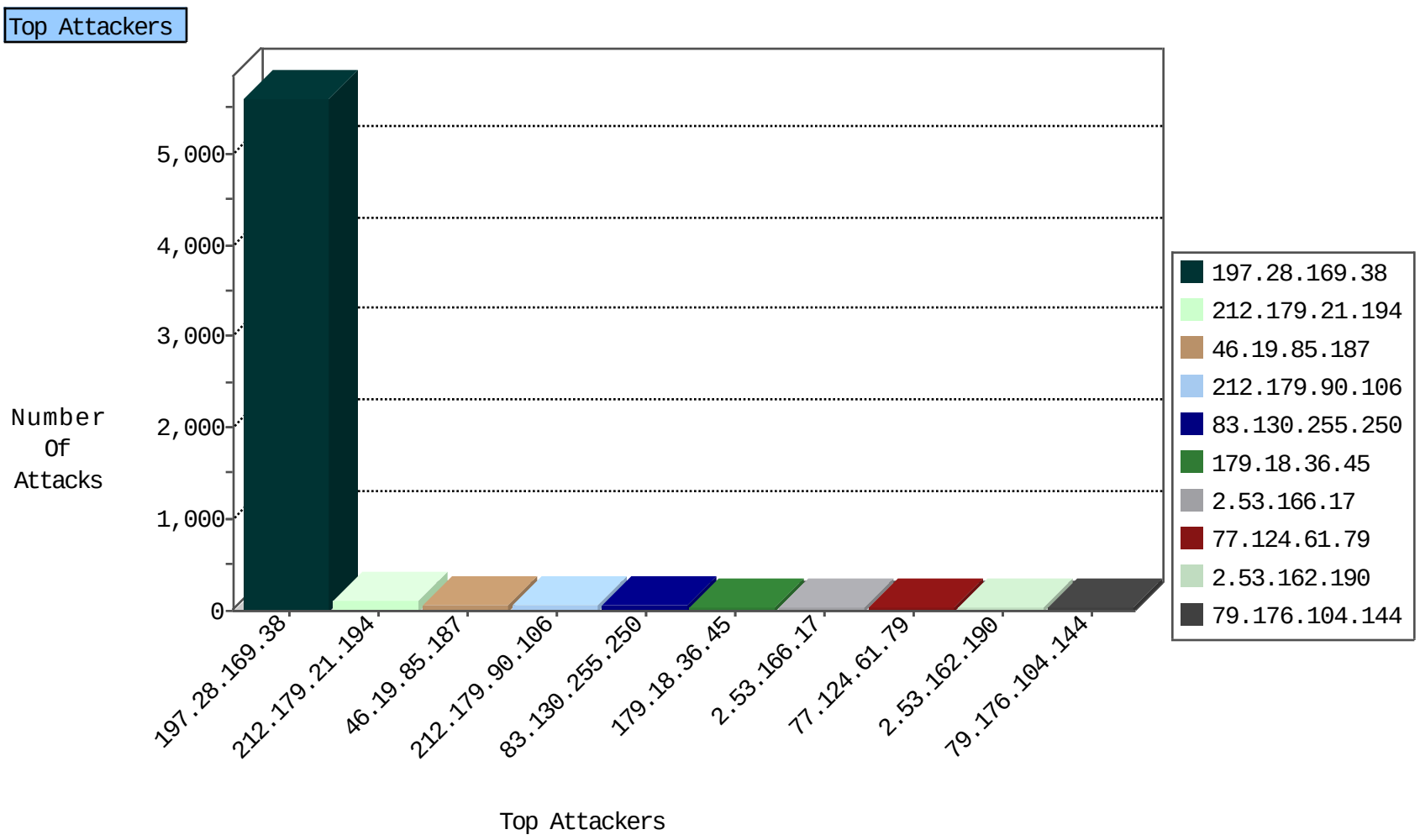
09-13-2016-14:04:00 to 09-13-2016-15:04:00

IDF Under Attack
Daily Report





09-13-2016-14:04:00 to 09-13-2016-15:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.128.20	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
197.28.169.38	Tunisia	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
220.189.255.9	China	147.237.0.33	idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.99	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
115.23.1.194	Korea, Republic of	147.237.0.17	m.my-kosher-kravi.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-13-2016-14:04:00 to 09-13-2016-15:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-13-2016-14:04:00 to 09-13-2016-15:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.177.227.200	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	6
197.28.169.38	147.237.77.216	Tunisia	dover.idf.il	portscan: TCP Distributed Portscan	2
2.53.145.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.80.155.255	147.237.77.74	United States	law.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	1
185.32.179.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.60.153.178	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.50	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.50	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
80.246.137.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
52.166.249.197	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
45.79.71.122	147.237.77.226	United States	www.chamatz.aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
212.179.159.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
115.23.1.194	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.50	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.50	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.132.136.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-13-2016-14:04:00 to 09-13-2016-15:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.28.169.38	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5302
197.28.169.38	Tunisia	147.237.77.216	dover.idf.il	SYN Attack		monitor	78
197.28.169.38	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	71
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
197.28.169.38	Tunisia	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN-ACK was acknowledged. Stripping all packet data.	drop	40
77.124.61.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
179.18.36.45	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
197.28.169.38	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	31
212.179.21.194	Israel	147.237.77.227	e.hamaz.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	29
83.130.255.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27
197.28.169.38	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	25
197.28.169.38	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
83.130.255.250	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
197.28.169.38	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
79.178.167.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
197.28.169.38	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
217.132.31.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
212.179.159.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.92	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	13
46.19.85.98	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
176.13.17.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.98	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.125	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	9
46.19.85.92	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
217.214.151.75	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.98	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
176.13.231.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
81.218.101.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.125	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.127	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
87.71.43.172	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
141.226.218.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
62.219.147.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.22.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.35.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
185.112.188.99	Iraq	147.237.76.177	ncore.idf.il	drop	First packet isn't SYN	drop	6
2.53.188.79	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
117.66.188.224	China	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
2.53.186.84	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
82.205.70.85	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

09-13-2016-14:04:00 to 09-13-2016-15:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
212.179.21.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	52
2.53.166.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
2.53.162.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
79.176.104.144	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.176.104.144	Block	17
79.176.104.144	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	16
27.154.34.210	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 27.154.34.210	Block	15
46.19.86.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
176.13.247.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
109.253.203.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
27.154.34.210	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	5
2.55.22.205	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	5
217.132.31.20	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
212.143.120.106	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	3
192.115.90.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.116.127.66	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/452-he/patzar.aspx	Block	2
2.53.3.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	2
89.139.105.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.53.162.190	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	2
46.19.86.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.53.165.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.108.193.30	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
68.180.229.41	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
109.67.63.192	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.55.33.4	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
79.177.222.92	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
176.110.62.15	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
85.64.145.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
77.138.218.189	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
217.132.44.28	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 217.132.44.28	Block	1
207.46.13.57	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
2.53.3.156	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
79.178.167.145	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.179.132.204	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.64.134	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.134	Block	1
179.18.36.45	Colombia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.68.44.232	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.96.21	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.143.91.166	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.240.236.119	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
152.62.109.208	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
80.246.133.186	Israel	147.237.76.42	refuah.idf.il	Distributed Suspicious Response Code	Block	1
213.57.105.224	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.64.134	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/m/main/giyus/general.aspx	Block	1
46.19.86.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
180.76.15.22	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/shared/clientscripts/{1}	Block	1
2.55.19.57	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1

09-13-2016-14:04:00 to 09-13-2016-15:04:00