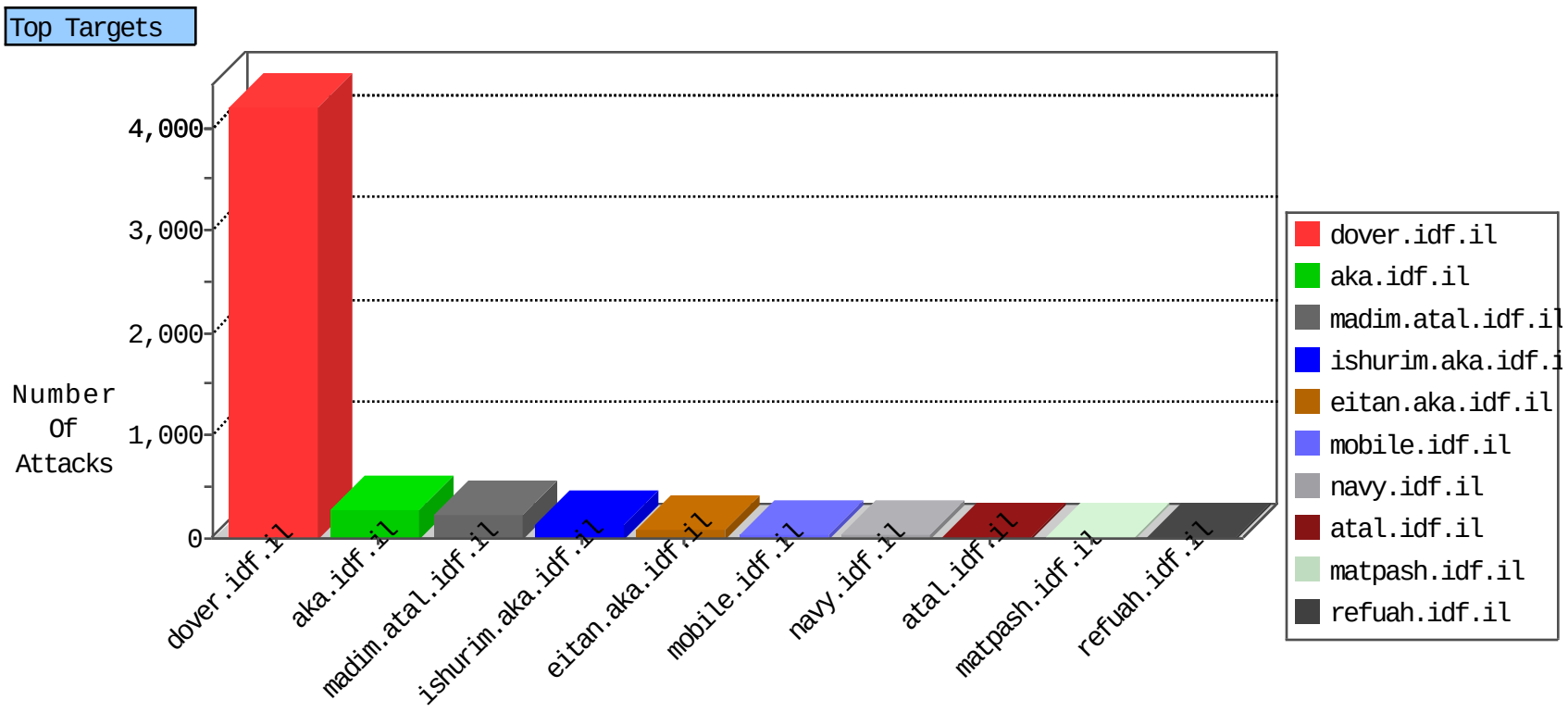
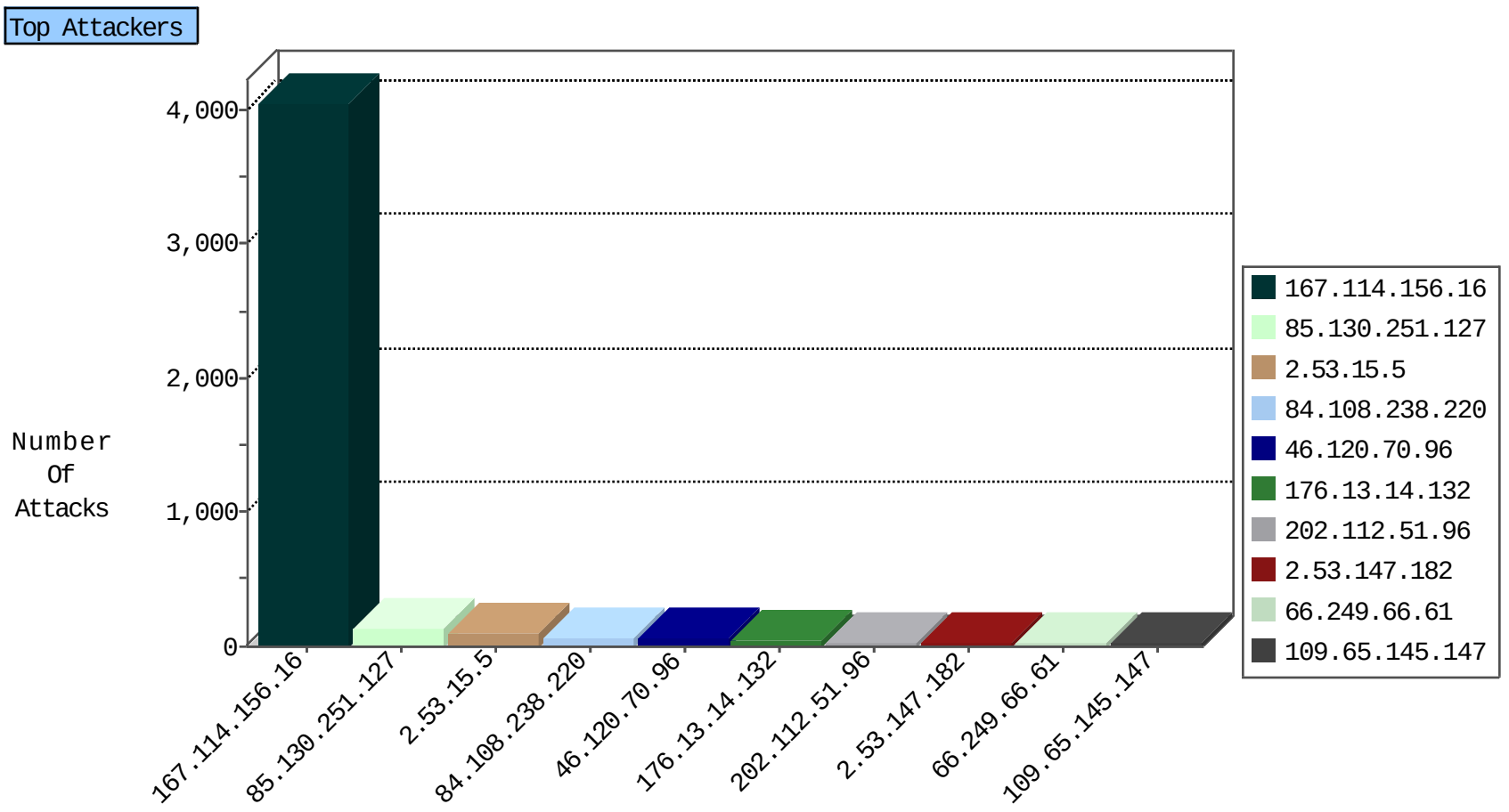
04-18-2016-20:04:08 to 04-18-2016-21:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-18-2016-20:04:08 to 04-18-2016-21:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4057
82.145.208.47	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	4
104.148.71.133	United States	147.237.8.14	e.orchot.idf.il	JLM_Purple_Con_Limit_Http	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
69.30.198.149	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	2
202.112.51.96	China	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	2
69.30.226.222	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	2
202.112.51.96	China	147.237.72.166	aka.idf.il	block-sp-traf1	forward	2
204.12.196.235	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
104.148.71.133	United States	147.237.8.14	e.orchot.idf.il	JLM_Under_Attack_Con_Http	drop	2
202.112.51.96	China	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
202.112.51.96	China	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
94.102.49.116	Netherlands	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
209.126.110.228	United States	147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1
209.126.110.228	United States	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1
82.145.211.140	Europe	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	1
79.177.93.52	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
209.126.110.228	United States	147.237.77.205	prisha.idf.il	Block_Udp_All_Nets	drop	1
82.145.223.143	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1
206.81.134.49	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
159.122.220.135	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

04-18-2016-20:04:08 to 04-18-2016-21:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.45.65.198	Egypt	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1

04-18-2016-20:04:08 to 04-18-2016-21:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.214	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.64.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
132.74.244.140	147.237.77.243	Israel	mobile.idf.il	ET SCAN NMAP -sA (2)	2
87.71.87.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.71.9.56	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.214.149.209	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 4096	1
104.214.149.209	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.158	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
87.71.30.51	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.102	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
79.176.95.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.99.142.35	147.237.0.34	Albania	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
104.214.149.209	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.158	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1

04-18-2016-20:04:08 to 04-18-2016-21:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.130.251.127	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	126
84.108.238.220	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	56
46.120.70.96	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	54
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
109.65.145.147	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
79.182.128.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.86.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
79.179.113.201	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.180.147.40	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	11
79.181.53.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
79.180.147.40	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
87.70.91.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.108.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.251.127	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
203.146.246.226	Thailand	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
88.226.129.206	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.2.171	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
80.246.130.214	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.235.224.91	Spain	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
77.127.127.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.180.147.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.30.24.4	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.242.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.65.114.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.16.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.124.5.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.130.214	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
94.230.86.191	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
87.71.89.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.155.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.149.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.101.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.62.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.125.80.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.186.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.179.121	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.206	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
79.177.216.95	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
84.109.113.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.132.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.181	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.159.169.211	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.242.94	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.55.179.121	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3

04-18-2016-20:04:08 to 04-18-2016-21:04:08

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.85.206	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.177.216.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3

04-18-2016-20:04:08 to 04-18-2016-21:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.15.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
176.13.14.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
2.53.147.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.85.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
109.253.225.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
109.253.225.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
79.181.98.82	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	7
109.253.225.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
80.246.133.11	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.246.133.11	Block	5
109.253.225.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
149.78.81.196	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	4
2.53.13.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
79.181.98.82	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.181.98.82	Block	3
109.65.145.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
78.137.12.238	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 78.137.12.238	Block	3
74.216.182.82	Canada	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 74.216.182.82	Block	3
2.53.185.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.114.105.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	2
109.253.225.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.235.224.91	Spain	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.133.11	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ???? in www.aka.idf.il/	None	1
202.112.51.96	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.paypal.com/	Block	1
74.216.182.82	Canada	147.237.77.176	matpash.idf.il	Unauthorized HTTP Method	Block	1
80.246.133.11	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ???? in www.aka.idf.il/main/home/default.aspx	None	1
66.249.66.182	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
185.27.105.182	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
80.246.133.11	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ???? in www.aka.idf.il/ishurim	None	1
202.112.51.96	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.paypal.com/	Block	1
74.216.182.82	Canada	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
52.16.137.212	Ireland	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to /	Block	1
80.246.139.138	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.181.98.82	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/	Block	1
69.30.198.149	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.app-softwares.com/	Block	1
185.103.252.5	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
80.246.133.11	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ???? in www.aka.idf.il/ishurim/	None	1
207.46.13.115	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
78.137.12.238	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/pniot.aspx'	Block	1
62.0.118.147	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/205-he/patzar.aspx	Block	1
87.70.91.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip storage/files/pdf	Block	1
80.82.65.82	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/shared/usercontrols/headerupper/	Block	1
69.30.226.222	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.369bs.com/	Block	1
2.53.188.217	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$btnSend.x in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
80.246.133.11	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ???? in www.aka.idf.il/ishurim/main	None	1
212.235.65.236	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.66.163	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/navmenu/	Block	1
197.45.65.198	Egypt	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
46.19.85.84	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
80.246.133.11	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ???? in www.aka.idf.il/ishurim/main/	None	1
213.57.210.12	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.66.180	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1

04-18-2016-20:04:08 to 04-18-2016-21:04:08