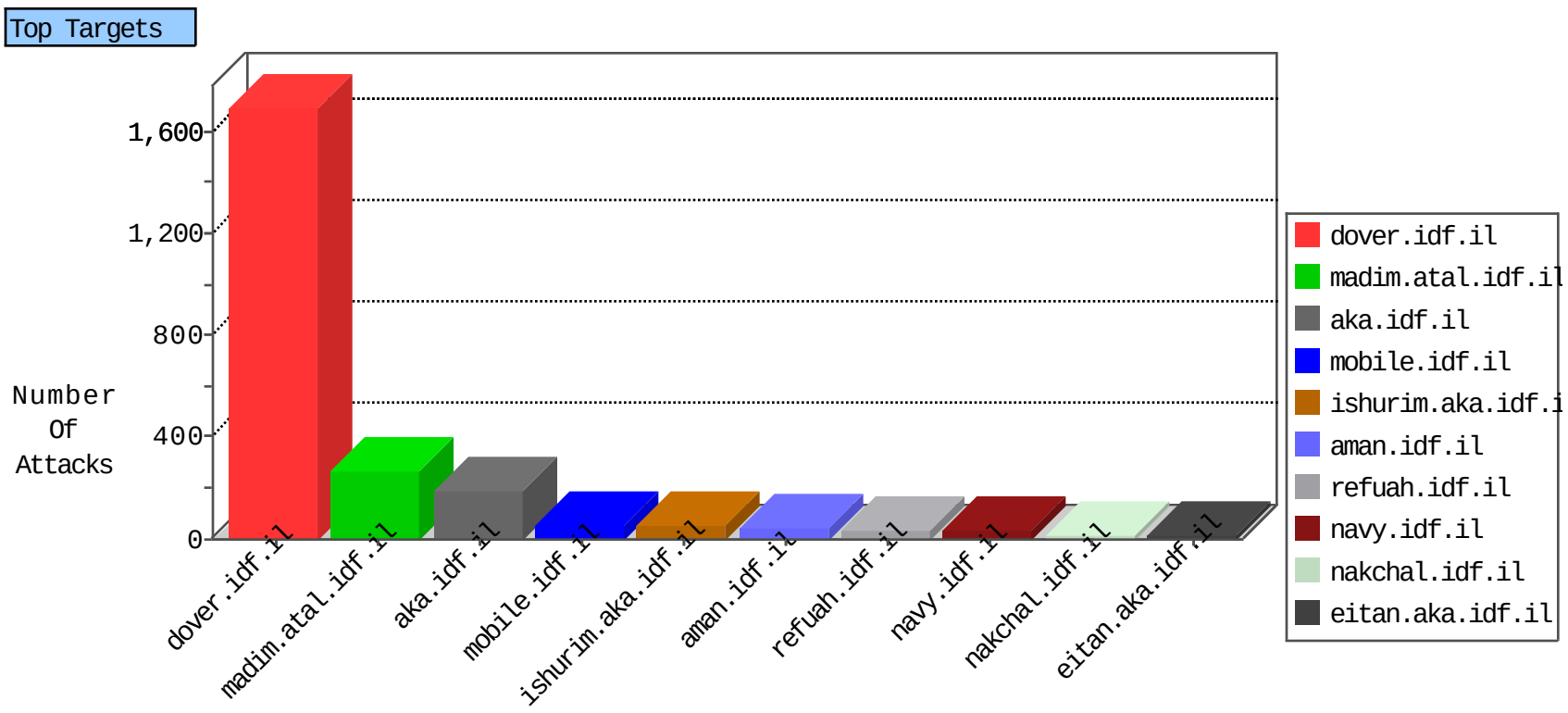
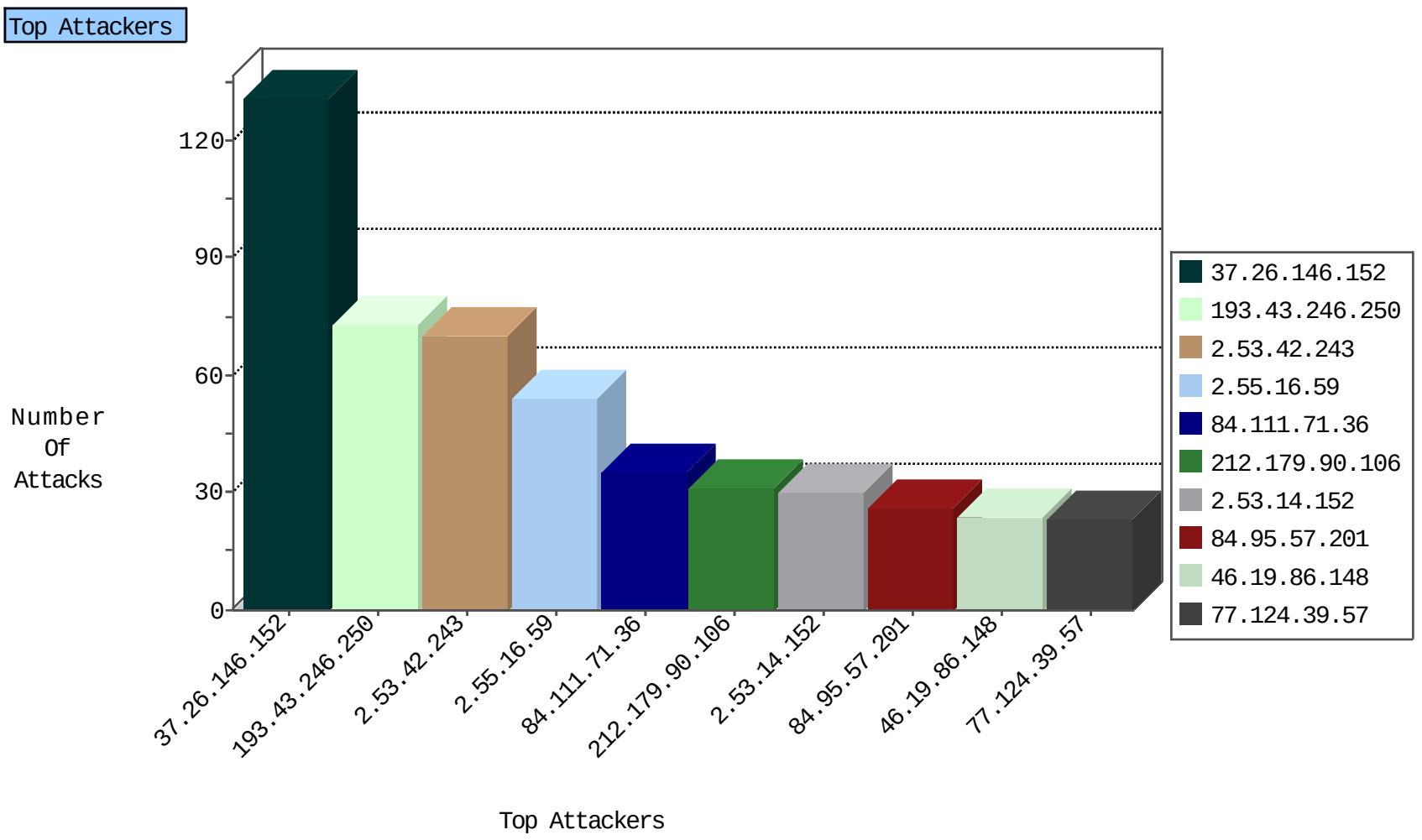
09-18-2016-16:04:08 to 09-18-2016-17:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-18-2016-16:04:08 to 09-18-2016-17:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.191.232.71	Israel	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	82
134.191.232.71	Israel	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Tcp	drop	32
155.64.138.28	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
110.249.208.86	China	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
37.26.149.211	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.35	Germany	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.118.78.199	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.86.139	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.110.125.52	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-18-2016-16:04:08 to 09-18-2016-17:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.68.118	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-18-2016-16:04:08 to 09-18-2016-17:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.160	147.237.72.156	Israel	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	7
222.254.34.165	147.237.0.19	Vietnam	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
77.126.62.99	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.89.37.88	147.237.77.178	Canada	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
46.121.79.148	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.238.45	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.148.187	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
128.199.207.123	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.29.169.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.98.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
92.29.69.152	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
85.130.141.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.118.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.254.34.165	147.237.0.33	Vietnam	idf.il	ET SCAN NMAP -sS window 1024	1
79.117.105.192	147.237.77.227	Romania	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
209.89.37.88	147.237.77.178	Canada	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
49.207.9.138	147.237.72.217	India	e.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.71.208.191	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
141.226.240.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.245.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.29.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.35.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.98.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.206.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.155.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-18-2016-16:04:08 to 09-18-2016-17:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
84.95.57.201	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	25
213.57.119.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
2.53.41.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
62.219.50.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.253.244.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
212.179.28.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
2.55.16.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
2.55.16.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
37.26.149.175	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
37.26.148.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.57	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
89.139.5.115	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
37.26.149.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
89.139.5.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.19.86.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.55.16.59	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
2.53.164.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.55.16.59	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
79.177.128.140	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.199.104.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
155.64.138.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.13.241.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.186.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.64.63.84	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
176.13.18.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.13.6.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
31.210.186.94	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.57	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.53.32.137	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
88.202.218.245	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.15.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.186.178	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.85.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.125.52.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.222.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.55.52.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.149.141	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
141.226.217.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.130.197.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

09-18-2016-16:04:08 to 09-18-2016-17:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
2.53.42.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
84.111.71.36	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 84.111.71.36	Block	33
46.19.86.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
46.19.86.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
46.19.86.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
5.29.254.39	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	5
77.124.39.57	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 77.124.39.57	Block	4
77.124.39.57	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 77.124.39.57	Block	4
212.25.84.200	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	4
77.124.39.57	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 77.124.39.57	Block	4
109.253.141.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.124.39.57	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 77.124.39.57	Block	3
46.19.86.195	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	3
77.139.108.51	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/klali.aspx	Block	3
46.19.85.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.164.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
76.21.116.21	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.111.71.36	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
109.253.199.127	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.55.27.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.75.7	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.178.75.7	Block	2
192.115.67.2	Israel	147.237.72.167	ishurim.aka.idf.i	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
46.19.86.53	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.55.54.53	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
79.178.75.7	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/home/giyus.	Block	1
180.7.113.102	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.19.85.182	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
77.138.192.133	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
2.53.164.42	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
195.60.235.57	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 195.60.235.57	Block	1
109.253.143.3	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.53.42.243	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
180.76.15.149	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/shared/clientscripts/jquery/' + url + '	Block	1
46.19.85.182	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method l/1256-he/Refuah.aspx in URL	Block	1
2.53.179.103	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
77.139.108.51	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	1
195.60.235.57	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/3203.jpg	Block	1
77.124.39.57	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
46.19.86.80	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
83.130.76.32	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
2.53.42.243	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.86.77.38	Ukraine	147.237.77.74	law.idf.il	Parameter Type Violation PageNum in www.law.idf.il/327-he/patzar.aspx	Block	1
54.161.51.139	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
89.139.222.224	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.139.222.224	Block	1
77.124.39.57	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version like Gecko) Chrome/53.0.2785.116 Safari/537.36	Block	1

09-18-2016-16:04:08 to 09-18-2016-17:04:08