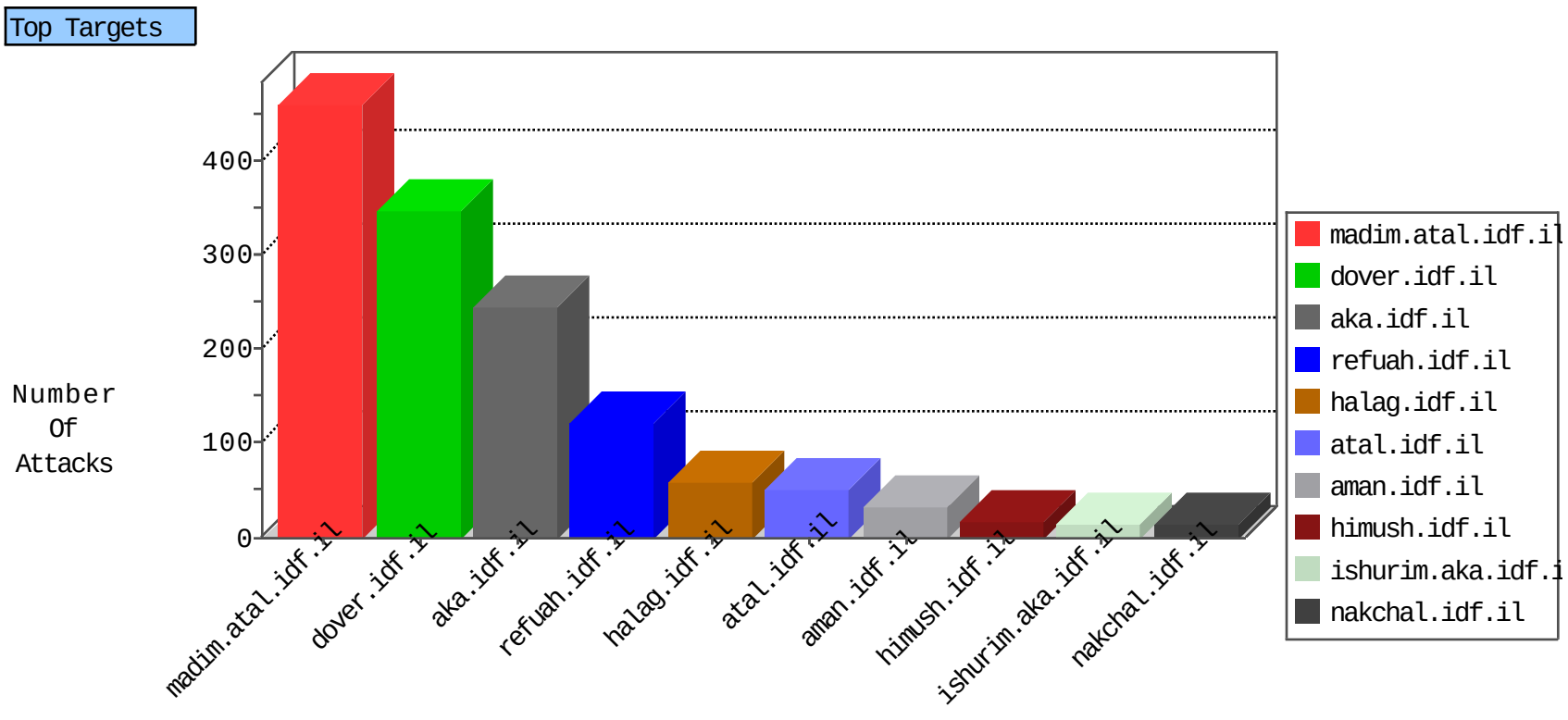
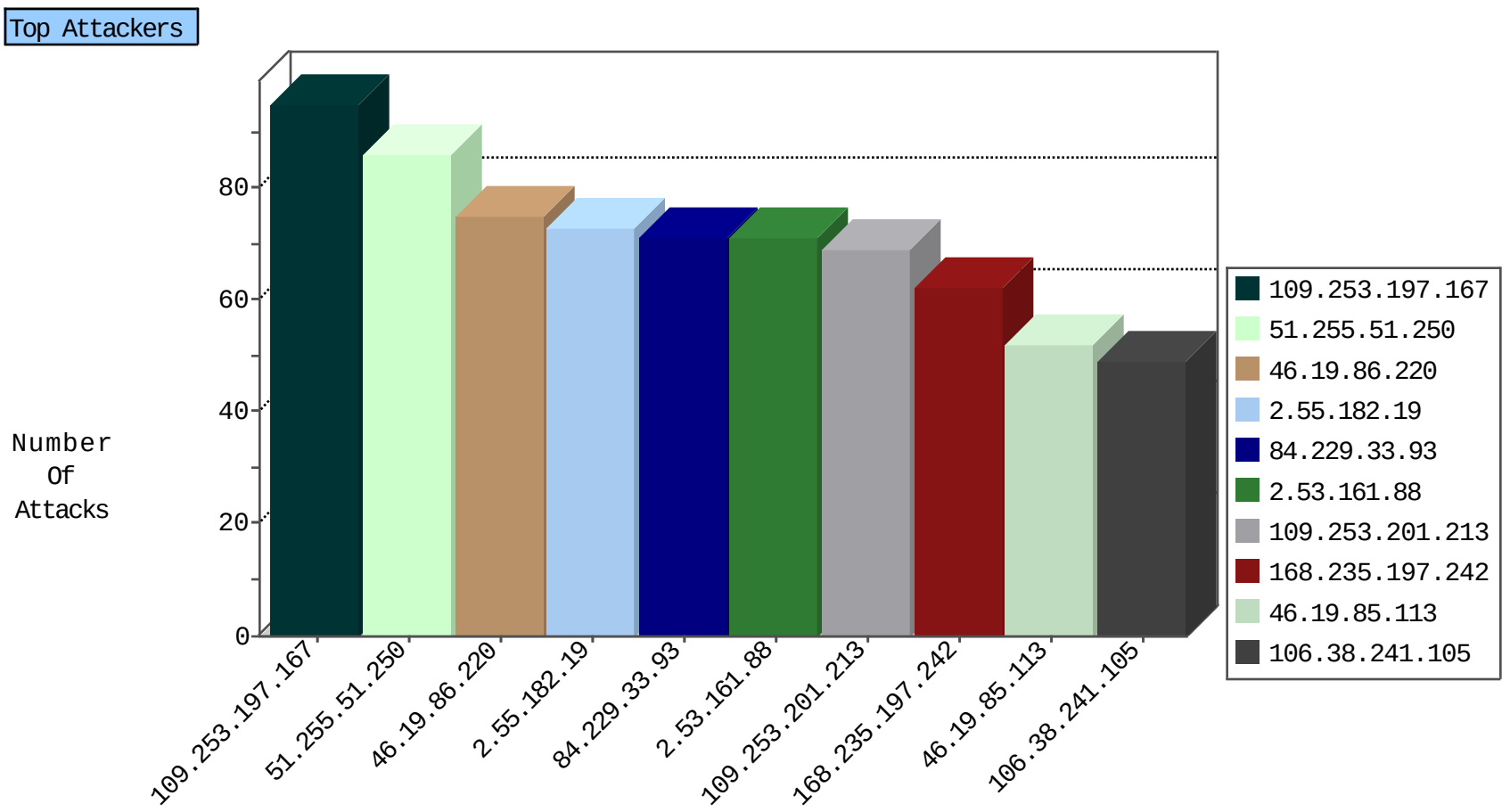
09-13-2016-10:04:09 to 09-13-2016-11:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-13-2016-10:04:09 to 09-13-2016-11:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
86.107.52.39	Romania	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
168.235.197.242	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	6
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.93.229.139	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	1
205.250.193.195	Canada	147.237.77.179	e.mazi.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.12	Ireland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
212.116.188.141	Israel	147.237.72.167	ishurim.aka.idf.il	Black List	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
109.64.186.91	Israel	147.237.8.46	e.chinuch.idf.il	Black List	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-13-2016-10:04:09 to 09-13-2016-11:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.51.250	France	147.237.77.234	halag.idf.il	C1000074: HTTP: majestic bot	Permit	53
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	36
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	12
51.255.51.250	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	10
51.255.51.250	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	8
51.255.51.250	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	5
51.255.51.250	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	4
51.255.51.250	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	4
51.255.51.250	France	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-13-2016-10:04:09 to 09-13-2016-11:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.182.20.121	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
185.110.132.201	147.237.76.201	Ukraine	e.atal.idf.il	ET SCAN Potential SSH Scan	1
79.181.205.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
50.116.123.135	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.158	147.237.77.235	Sweden	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
172.245.173.142	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.158.203.147	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.249.220.50	147.237.77.216	Lebanon	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.83.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.76.107.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.115.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.145.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.88.157.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.6.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
79.178.132.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
50.116.123.135	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.89.217.232	147.237.72.166	Netherlands	aka.idf.il	portscan: TCP Distributed Portscan	1
46.227.67.158	147.237.77.234	Sweden	halag.idf.il	ET SCAN NMAP -sS window 1024	1
151.11.201.3	147.237.72.167	Italy	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.85.101	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.208.139.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.79.103.178	147.237.77.216	United States	dover.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
213.57.223.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.171.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.0.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.25.66.96	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.198.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.189.125	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.90.25.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.195.147	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-13-2016-10:04:09 to 09-13-2016-11:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
84.229.33.93	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	70
168.235.197.242	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	56
109.253.197.167	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.95	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
46.19.85.95	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
62.0.237.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	19
62.0.213.129	Israel	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	18
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
62.0.213.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
217.194.206.38	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
87.69.36.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
87.69.36.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
87.69.36.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
46.19.85.226	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	11
130.193.51.3	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
80.178.101.40	Israel	147.237.72.166	aka.idf.il	SYN Attack		monitor	9
80.178.101.40	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.253.87.115	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
86.107.52.39	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.178.230.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
217.132.141.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.156	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.156	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.244.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.178.101.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
213.57.70.7	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.8	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.53.129.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.8	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.0.200.213	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.225.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
94.226.196.174	Belgium	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.154	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
176.13.232.22	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
176.13.232.22	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
62.0.213.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
81.218.159.104	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
185.3.147.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.226	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
176.13.246.211	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	3
46.19.86.245	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.30.189	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	3

09-13-2016-10:04:09 to 09-13-2016-11:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.182.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
46.19.86.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
109.253.197.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
109.253.201.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
2.53.161.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
46.19.85.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
62.0.41.2	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	10
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
79.182.33.218	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
79.183.33.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.0.41.2	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/4/	Block	3
2.55.61.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.178.181	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
213.87.147.90	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	3
46.19.86.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.215.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.161.88	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
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	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
81.218.251.252	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.251.252	Block	2
176.13.236.9	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	1
84.229.33.93	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
31.168.216.122	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.56.49	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/milluim/index	Block	1
217.64.86.6	Germany	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method [[#21]][[#3]][[#3]][[#0]]0£øEYý±%Í®p[[#30]]*å[[#25]]‰V›w[[#23]]äŽ¼[[#5]]d'üCAM8Ï,{Ù@Ž¯Å in URL	Block	1
212.25.79.133	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
46.19.85.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.202.103	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
2.53.190.84	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.64.86.6	Germany	147.237.77.216	dover.idf.il	Multiple NULL Character in Method from 217.64.86.6	Block	1
81.218.251.252	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/guyus	Block	1
77.125.14.53	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
217.64.86.6	Germany	147.237.77.176	matpash.idf.il	Abnormally Long Request method	Block	1
176.13.244.253	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.66.132.18	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
37.26.148.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.64.86.6	Germany	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name	Block	1
80.246.130.150	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
212.199.57.192	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
81.218.251.252	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
217.64.86.6	Germany	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 217.64.86.6	Block	1
77.139.171.0	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
217.64.86.6	Germany	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in Method [[#21]][[#3]][[#3]][[#0]]0£øEYý±%Í®p[[#30]]*å[[#25]]‰V›w[[#23]]äŽ¼[[#5]]d'üCAM8Ï,{Ù@Ž¯Å	Block	1
203.117.143.129	Singapore	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/miluim/templates/inner.asp	Block	1
109.253.157.129	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
37.26.149.152	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
217.64.86.6	Germany	147.237.77.216	dover.idf.il	Malformed URL	Block	1

09-13-2016-10:04:09 to 09-13-2016-11:04:09