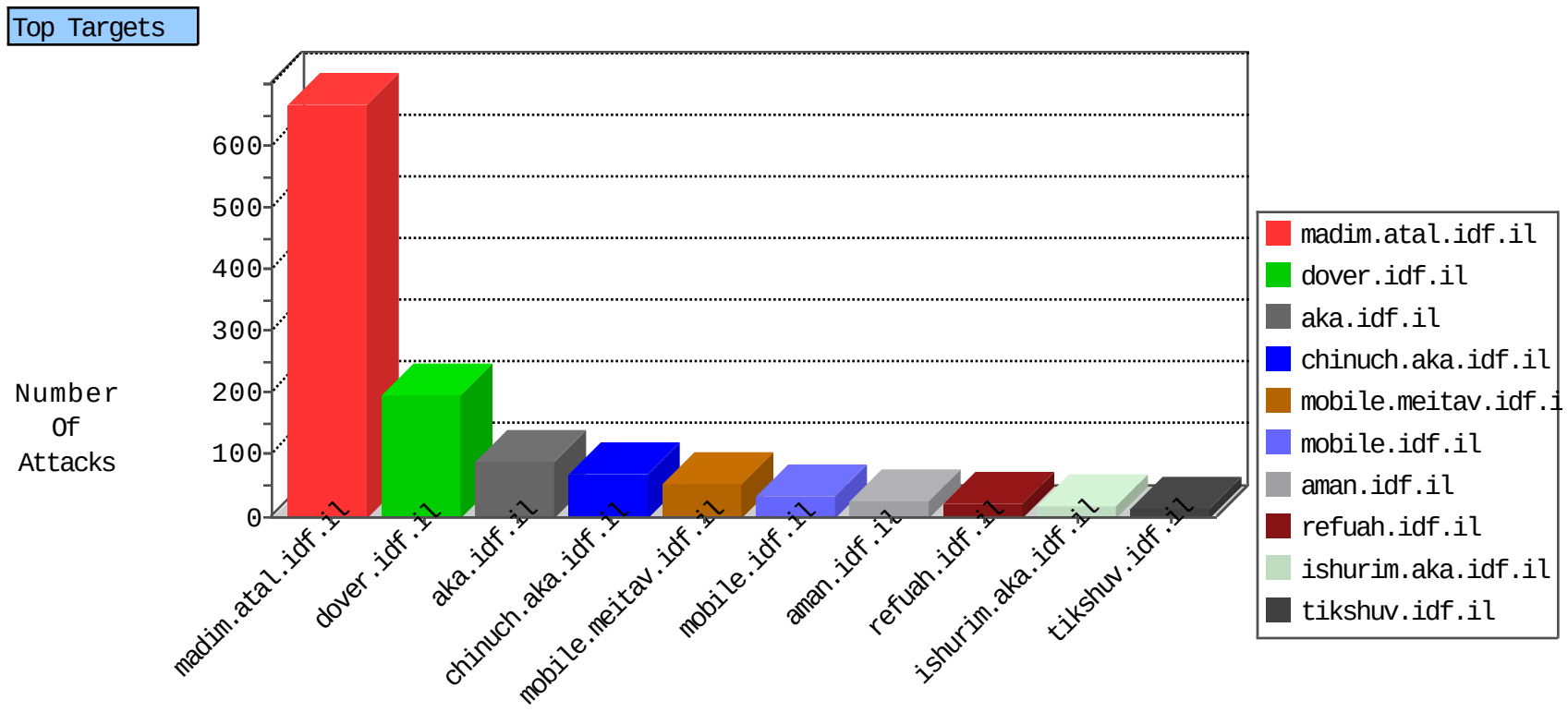
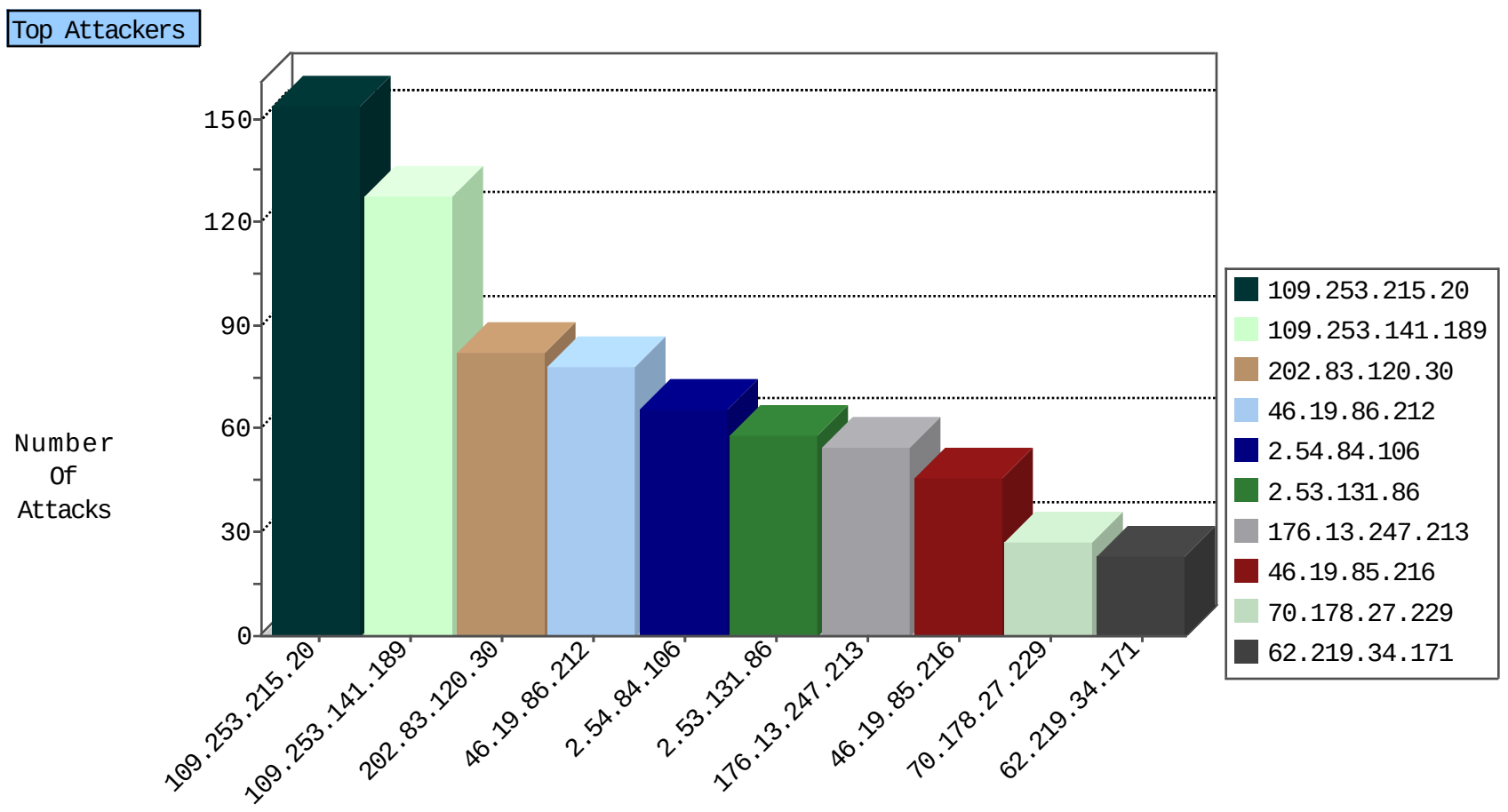
09-25-2016-13:04:05 to 09-25-2016-14:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-25-2016-13:04:05 to 09-25-2016-14:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.146.125	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
193.169.70.109	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
212.25.74.130	Israel	147.237.77.216	dover.idf.il	Black List	drop	4
31.168.133.226	Israel	147.237.72.167	ishurim.aka.idf.il	Black List	drop	3
212.25.74.130	Israel	147.237.72.167	ishurim.aka.idf.il	Black List	drop	3
213.151.43.188	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
81.218.165.186	Israel	147.237.77.216	dover.idf.il	Black List	drop	3
196.105.233.2	Kenya	147.237.77.216	dover.idf.il	block-sp-traf1	forward	2
78.129.171.175	United Kingdom	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
45.121.230.177	India	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
78.129.171.175	United Kingdom	147.237.76.197	e.himush.idf.il	Black List	drop	1
50.30.37.27	United States	147.237.76.30	himush.idf.il	Black List	drop	1
208.67.1.248	United States	147.237.76.176	test.ncore.idf.il	Black List	drop	1
50.30.37.27	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1

09-25-2016-13:04:05 to 09-25-2016-14:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.138.2.243	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.206	United States	147.237.77.234	halag.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.143.245	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	1
62.210.143.245	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	1
69.30.213.82	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1

09-25-2016-13:04:05 to 09-25-2016-14:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.144.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.47.165.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.138.25.237	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.242.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
141.226.161.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.46.39.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.226.22.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.49.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.161.75	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.118.124	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.252.122	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.135.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.177.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.138.165.149	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
188.146.5.148	147.237.77.216	Poland	dover.idf.il	portscan: TCP Distributed Portscan	1
71.15.85.176	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
141.226.161.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.63.28.189	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
117.1.221.31	147.237.77.216	Vietnam	dover.idf.il	portscan: TCP Distributed Portscan	1
31.211.102.129	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
89.139.108.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.57.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.193.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.98.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.164.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-25-2016-13:04:05 to 09-25-2016-14:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
62.219.34.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
66.249.93.83	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
62.0.200.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	10
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
62.0.200.219	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	10
62.219.34.171	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	10
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	8
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	8
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
62.0.200.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
83.130.221.249	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	6
176.13.3.63	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.33.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.141.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.19.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.130.250.224	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
109.253.141.189	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
70.178.27.229	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.86.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
70.178.27.229	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
37.26.147.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
185.137.19.76		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.2.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.138	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
188.126.80.7	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.103	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
70.178.27.229	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
70.178.27.229	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
70.178.27.229	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
85.130.250.224	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
213.57.119.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.161.168	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.182.98.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
70.178.27.229	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
37.26.147.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.214	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
70.178.27.229	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.235.50.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

09-25-2016-13:04:05 to 09-25-2016-14:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.215.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	154
109.253.141.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
46.19.86.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
2.54.84.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
2.53.131.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
176.13.247.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
46.19.85.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
80.246.136.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
37.26.148.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
2.53.154.158	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	13
46.19.86.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
192.114.181.130	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.114.181.130	Block	9
46.19.86.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
176.13.19.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.86.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
213.151.35.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.114.181.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/5/	Block	3
80.246.137.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.151.35.214	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.151.35.214	Block	3
46.210.233.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.167.253	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
2.55.33.54	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.55.57.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.199.69.1	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
46.19.86.14	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
213.151.35.214	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/	Block	2
31.168.21.80	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
109.253.141.189	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.102.9.3	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
212.150.189.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl23 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
95.86.69.11	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
2.53.141.174	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.57.7.4	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	1
77.138.243.23	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
217.194.202.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/guyus	Block	1
66.102.9.6	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
212.179.21.192	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.247.118	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
2.53.154.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
109.67.205.240	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
77.139.11.118	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	1
192.115.200.57	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Abnormally Long Request method	Block	1
81.218.118.124	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 81.218.118.124	Block	1
217.194.202.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/guyus	Block	1
66.249.66.239	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/7/3097.pdfý	Block	1
109.253.136.139	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
79.179.192.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.117.173.57	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1

09-25-2016-13:04:05 to 09-25-2016-14:04:05