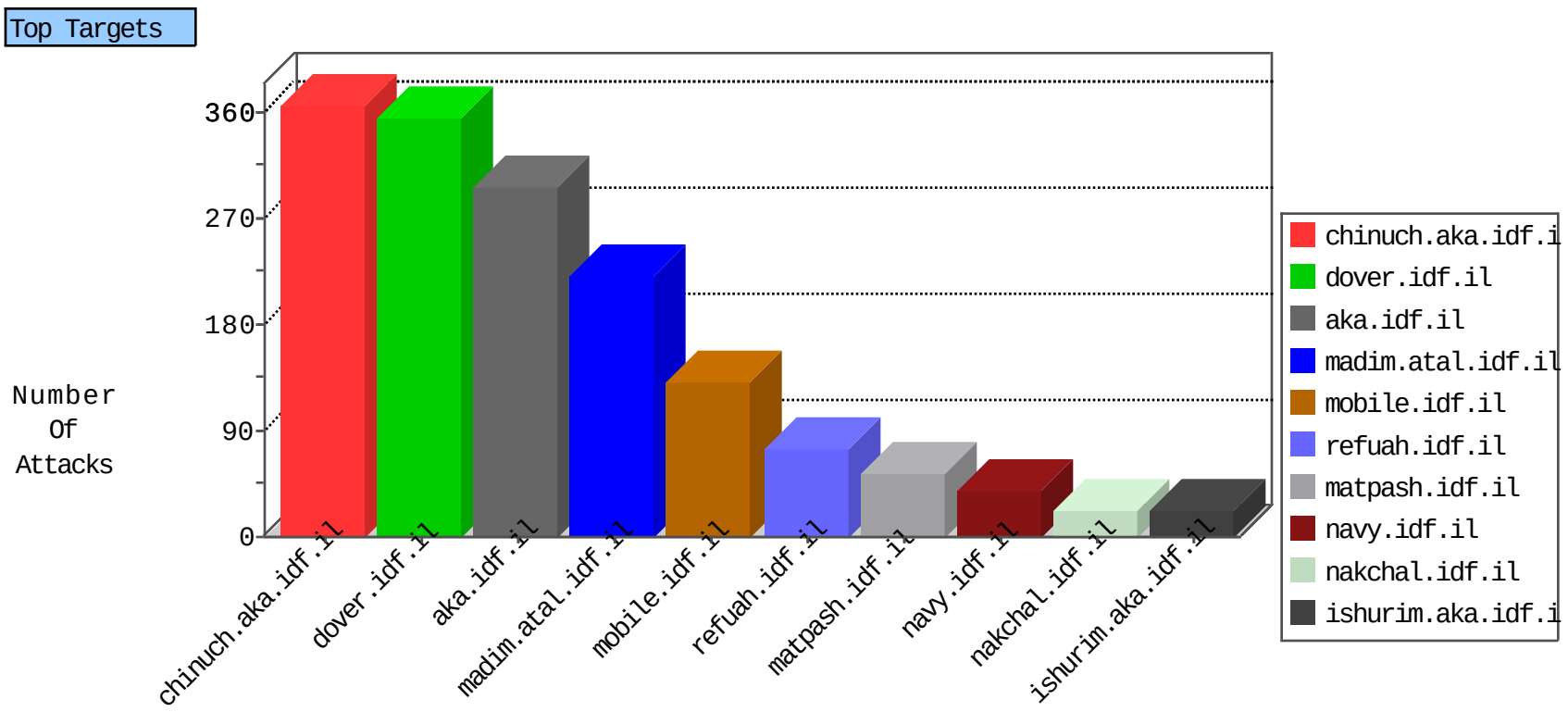
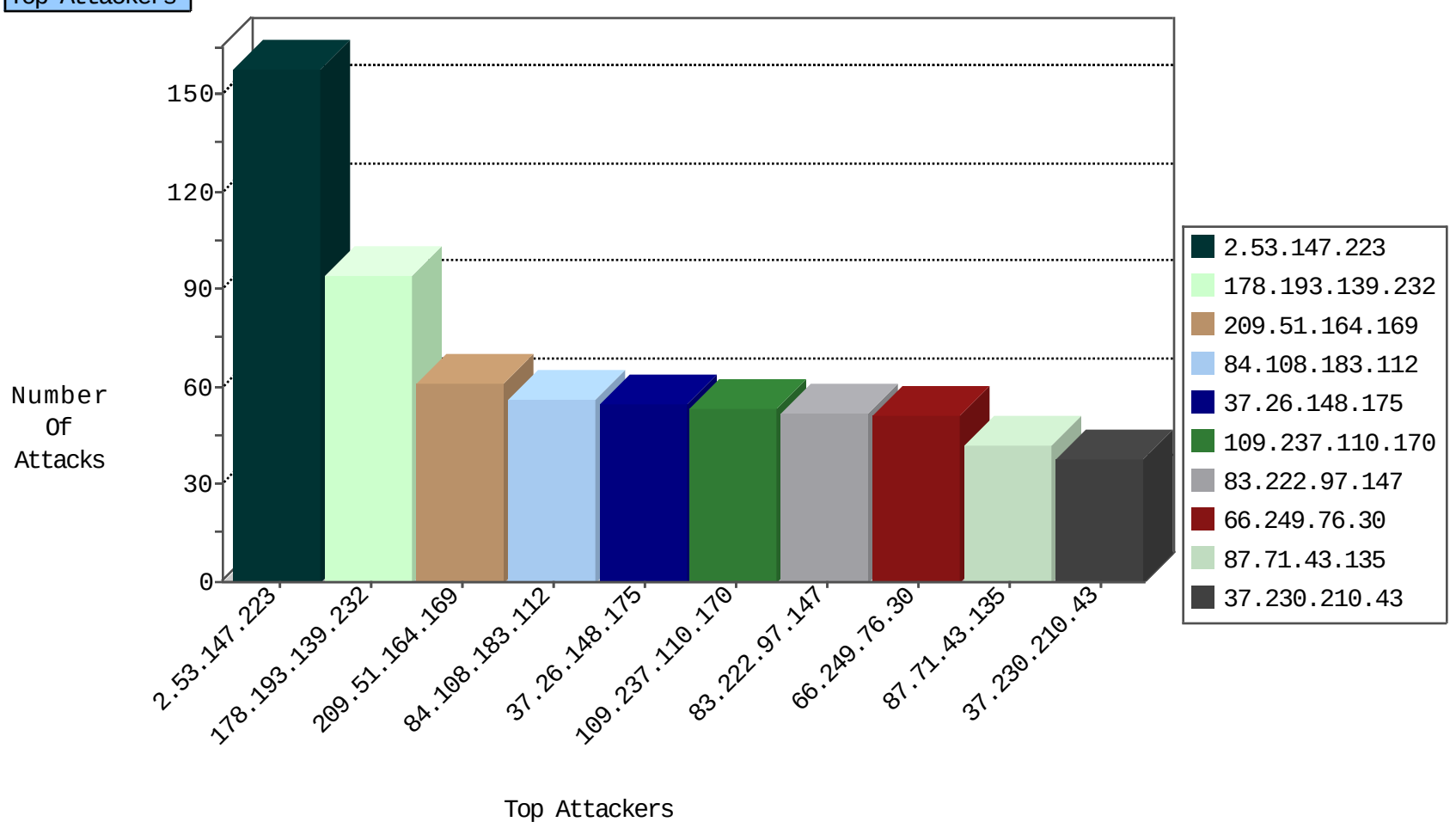
09-27-2016-15:04:09 to 09-27-2016-16:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-27-2016-15:04:09 to 09-27-2016-16:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.183.112	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	29
109.253.210.173	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
41.227.82.219	Tunisia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	7
209.126.136.2	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
196.200.16.201	Kenya	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
69.30.227.219	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
41.206.63.132	Kenya	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
196.200.16.202	Kenya	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
69.30.227.220	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
173.208.198.11	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
41.206.63.133	Kenya	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
196.200.16.203	Kenya	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
79.181.207.43	Israel	147.237.72.166	aka.idf.il	Black List	drop	1
176.13.229.15	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-27-2016-15:04:09 to 09-27-2016-16:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.135.8.175	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.213.138	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-27-2016-15:04:09 to 09-27-2016-16:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.86.56	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.230.86.16	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.206.13.166	147.237.76.39	Nigeria	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.158	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -f -sS	1
2.53.185.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.5.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.149.222.5	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.188.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.149.222.5	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
202.155.58.28	147.237.0.19	Indonesia	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.161.40.17	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
151.37.26.183	147.237.77.216	Italy	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.165.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
103.210.32.3	147.237.72.166		aka.idf.il	portscan: TCP Distributed Portscan	1
41.231.22.165	147.237.72.167	Tunisia	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
37.26.147.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.229.29.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.29.202.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.9.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.149.222.5	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.148.115.22	147.237.77.216	China	dover.idf.il	GPL SCAN nmap TCP	1
211.149.222.5	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
163.172.238.45	147.237.8.27	United Kingdom	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.117.45.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
113.240.250.154	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.156	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.177.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

09-27-2016-15:04:09 to 09-27-2016-16:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.76.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
87.71.43.135	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	41
66.249.64.163	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	20
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	19
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
209.51.164.169	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	18
209.51.164.169	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	17
209.51.164.169	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	16
109.253.138.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
91.135.102.164	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
80.178.218.176	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
176.13.13.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.237.110.170	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	12
109.237.110.170	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
212.235.98.139	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	12
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.237.110.170	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	11
83.222.97.147	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	11
83.222.97.147	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	11
80.246.140.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
83.222.97.147	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
109.237.110.170	Russian Federation	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
84.108.183.112	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
83.222.97.147	Russian Federation	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
46.19.86.47	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
83.222.97.147	Russian Federation	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
37.26.148.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.19.85.70	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.31	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
66.249.76.31	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.81.48.89	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
209.51.164.169	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.85.31	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
85.64.8.175	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.86.47	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.86.108	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
109.237.110.170	Russian Federation	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
37.26.148.175	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.70	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
79.178.0.119	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
37.26.148.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.178.54.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
62.0.214.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.148.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
5.22.134.207	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

09-27-2016-15:04:09 to 09-27-2016-16:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.147.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	154
37.26.147.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
112.111.173.122	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 112.111.173.122	Block	17
46.121.115.171	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.121.115.171	Block	9
112.111.173.122	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	7
109.253.197.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
2.53.178.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
77.139.20.137	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.13.16.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
132.64.217.142	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	4
109.65.138.229	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.65.138.229	Block	4
109.253.221.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.185.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.0.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	3
192.198.151.45	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	3
2.53.159.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.40.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.157.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.150	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
77.138.92.169	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	2
147.236.38.204	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 147.236.38.204	Block	2
37.26.149.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
78.40.225.156	Turkey	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/8/70768.jpg	Block	1
37.26.147.155	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
66.249.93.158	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
62.99.25.95	Spain	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/español	Block	1
46.19.85.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.139.221	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunsummary.aspx	Block	1
192.117.255.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
132.64.217.142	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 132.64.217.142	Block	1
46.19.85.197	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.65.138.229	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
78.46.23.198	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
176.13.235.197	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
66.102.6.21	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
81.218.70.243	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/browserconfig.xml	Block	1
192.198.151.45	Europe	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim	Block	1
77.139.85.185	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim	Block	1
66.249.69.104	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
132.64.217.142	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	1
109.253.136.71	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
46.19.86.56	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/favicon.ico	Block	1
37.26.147.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
185.27.106.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
77.126.86.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-27-2016-15:04:09 to 09-27-2016-16:04:09