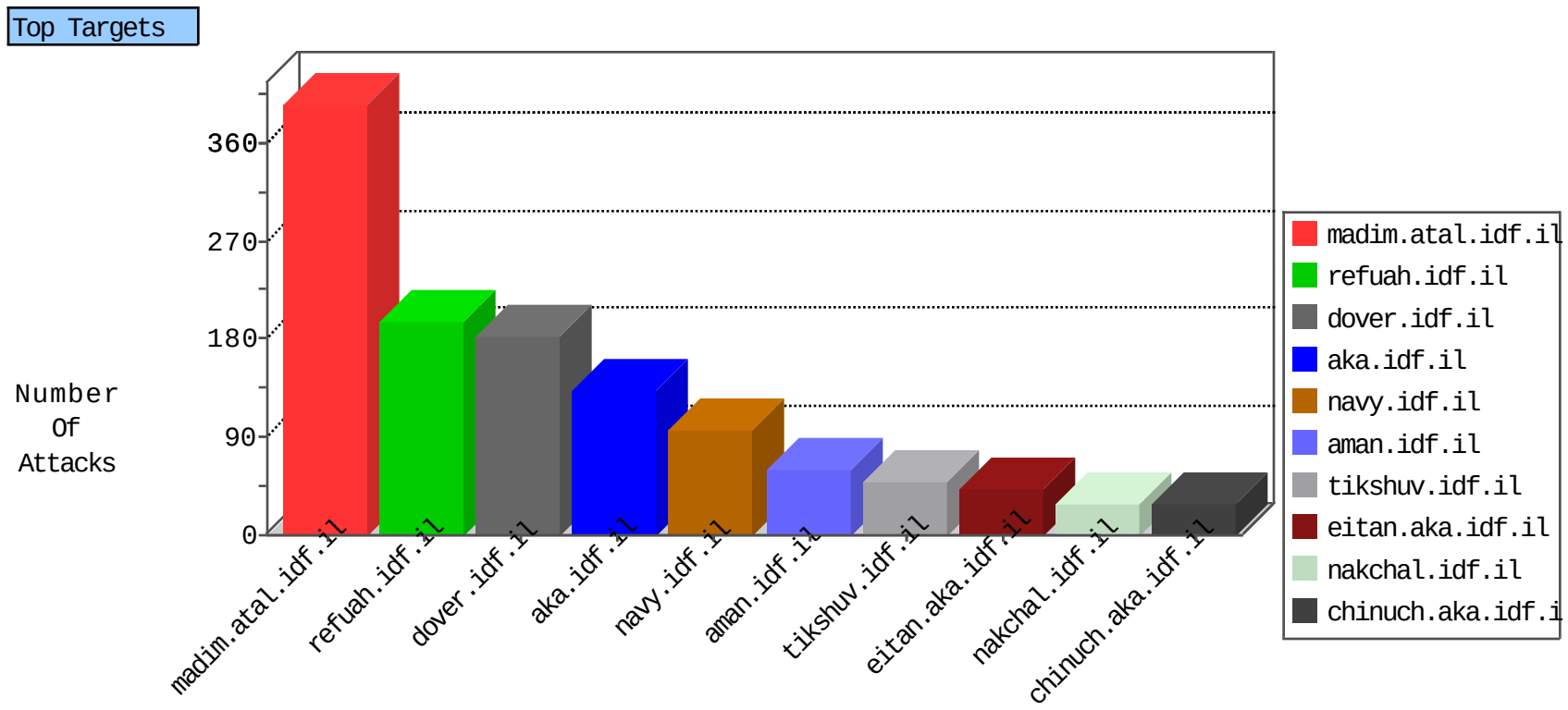
09-10-2016-17:04:09 to 09-10-2016-18:04:09

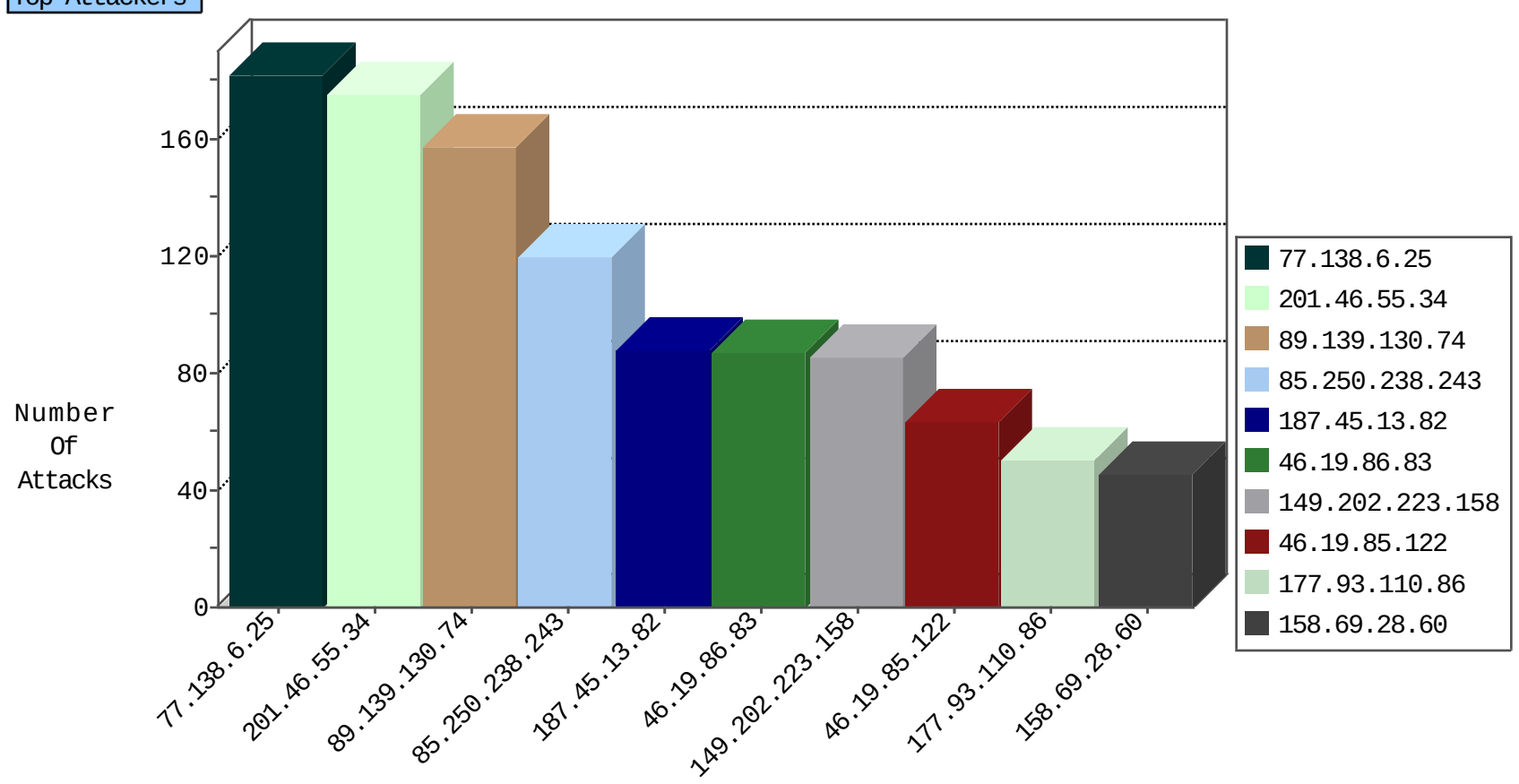
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-10-2016-17:04:09 to 09-10-2016-18:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.219.172.175	Morocco	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
120.132.50.135	China	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
37.48.77.131	Netherlands	147.237.76.201	e.atal.idf.il	Black List	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-10-2016-17:04:09 to 09-10-2016-18:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.198.202	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.198.202	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
179.43.141.208	Switzerland	147.237.76.147	chinuch.aka.idf.il	34161: ICMP: Communication with Destination Host is Administratively Prohibited (Code 10)	Block	1
71.6.135.131	United States	147.237.0.17	m.my-kosher-kravi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
85.65.121.109	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-10-2016-17:04:09 to 09-10-2016-18:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
211.141.78.56	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
104.148.120.134	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
198.58.110.199	147.237.77.74	United States	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.148.120.134	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
117.135.131.60	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.76.202	Canada	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
107.155.25.135	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
103.207.39.82	147.237.76.86	Vietnam	navy.idf.il	ET SCAN NMAP -sS window 1024	1
107.155.25.135	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
37.48.93.217	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	1
107.155.25.135	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
37.48.93.217	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
107.155.25.135	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
37.48.93.217	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
107.155.25.135	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
104.148.120.134	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
211.141.78.56	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
104.148.120.134	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
191.111.133.24	147.237.77.205	Colombia	prisha.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.148.120.134	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.123.101.31	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
103.255.47.41	147.237.77.205	Hong Kong	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
107.155.25.135	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.251	147.237.72.166	United States	aka.idf.il	WEB-CGI redirect access	1
107.155.25.135	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
37.48.93.217	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
107.155.25.135	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
37.48.93.217	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
107.155.25.135	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
37.48.93.217	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
107.155.25.135	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

09-10-2016-17:04:09 to 09-10-2016-18:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.139.130.74	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	150
46.19.86.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
46.19.86.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
46.19.86.83	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
46.19.86.83	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
87.69.36.34	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
46.19.86.184	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
79.182.114.79	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.121	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	13
201.46.55.34	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
201.46.55.34	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.34	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.34	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.34	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.34	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.34	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.34	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.34	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.34	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.34	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.34	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
149.202.223.158	France	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.34	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.34	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.34	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.34	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
149.202.223.158	France	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.34	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.34	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
79.177.239.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
149.202.223.158	France	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.34	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
108.61.239.202	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
149.202.223.158	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
149.202.223.158	France	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
105.225.117.172	South Africa	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
149.202.223.158	France	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.34	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
187.45.13.82	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
176.13.248.150	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
201.46.55.34	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
77.139.241.166	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
149.202.223.158	France	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
187.45.13.82	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
79.182.114.79	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
149.202.223.158	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
5.29.175.58	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
187.45.13.82	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
187.45.13.82	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
201.46.55.34	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5

09-10-2016-17:04:09 to 09-10-2016-18:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.138.6.25	France	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	182
85.250.238.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	120
46.19.85.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
183.14.17.241	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 183.14.17.241	Block	17
46.121.252.215	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	9
37.26.148.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
77.139.215.3	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	6
183.14.17.241	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
217.132.155.55	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sviva	Block	3
2.55.158.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
62.210.172.226	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	2
79.179.60.4	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	2
88.198.230.173	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	2
183.14.17.241	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
144.76.4.145	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	1
2.53.48.61	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.93.87	Israel	147.237.77.216	dover.idf.il	Distributed URL is Above Root Directory	Block	1
157.55.39.227	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
62.210.89.12	France	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	1
88.198.52.114	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	1
5.29.175.58	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.139.13.52	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
62.210.178.238	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	1
204.79.180.170	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
144.76.27.230	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	1
79.180.137.16	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 79.180.137.16 (Open Mode)	None	1
2.53.48.61	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/milluim/index	Block	1
176.9.10.108	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	1
62.210.89.20	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	1
66.102.8.217	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
204.79.180.183	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
62.210.82.112	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	1
144.76.32.51	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	1
79.180.137.16	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
2.53.59.98	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
77.138.17.182	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1
62.210.89.61	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	1
46.4.15.197	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.4.15.197	Block	1
89.139.130.74	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
78.46.89.51	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	1
66.249.64.36	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1264-he/refuah.aspx	Block	1
144.76.39.169	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	1
62.210.82.177	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	1
79.180.210.248	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	1
2.53.132.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
77.138.153.54	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.153.54	Block	1
62.210.172.99	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	1
46.4.15.197	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
109.186.76.154	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
79.178.201.159	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1

09-10-2016-17:04:09 to 09-10-2016-18:04:09