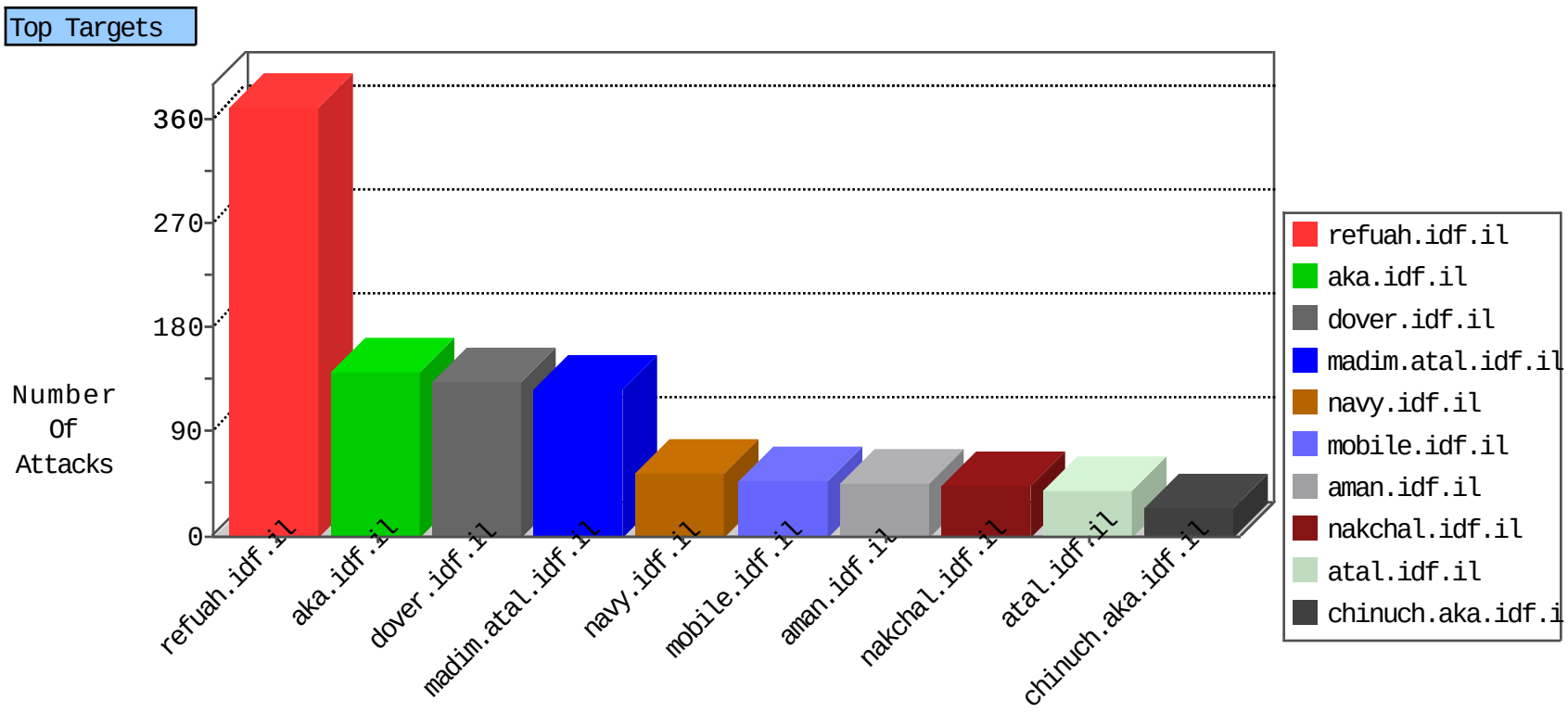
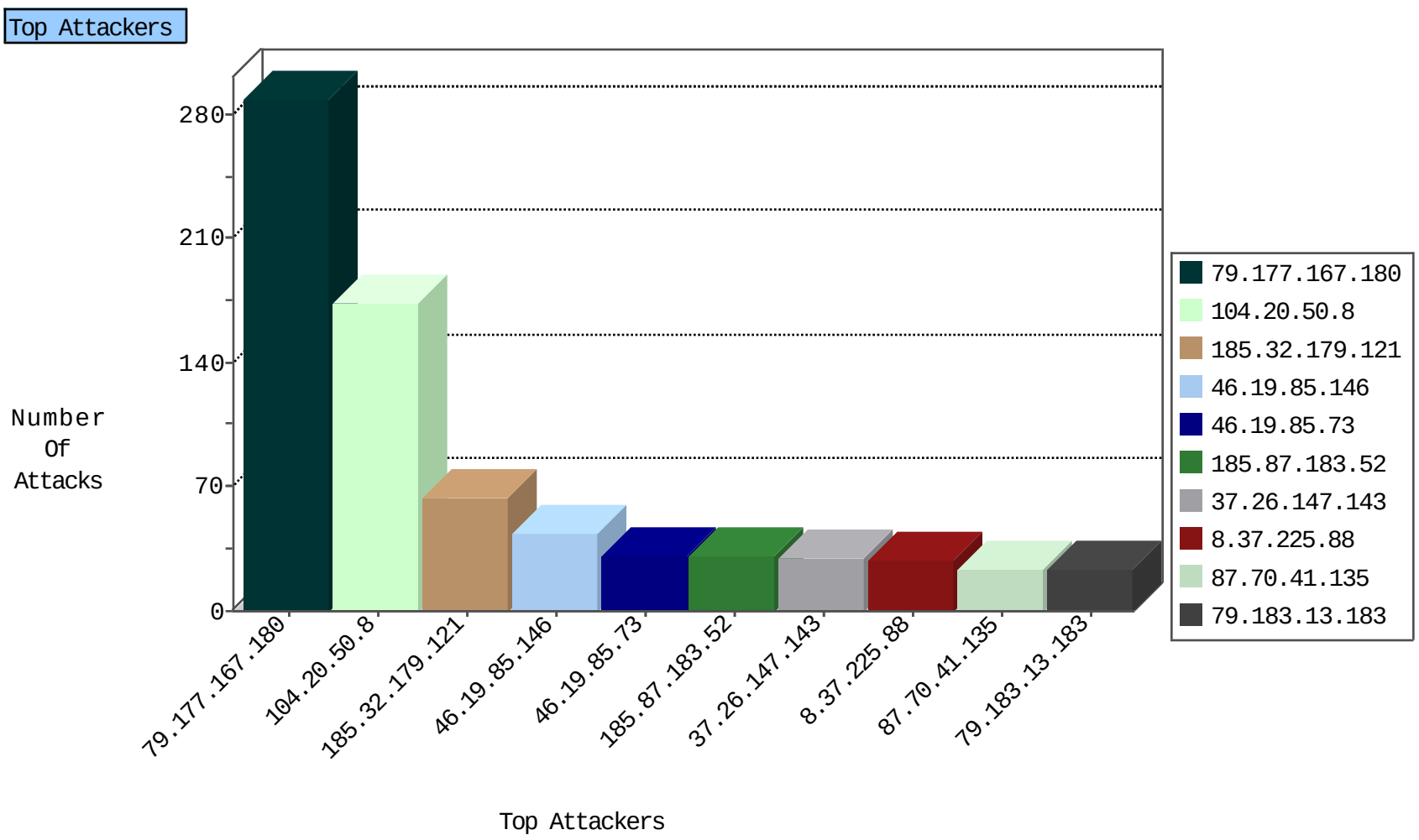
09-09-2016-13:04:08 to 09-09-2016-14:04:08

IDF Under Attack Daily Report





09-09-2016-13:04:08 to 09-09-2016-14:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.197	e.himush.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.201	e.atal.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.202	e.halag.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	2
179.99.200.39	Brazil	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	1
191.96.249.34	Chile	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

09-09-2016-13:04:08 to 09-09-2016-14:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.162.166	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3

09-09-2016-13:04:08 to 09-09-2016-14:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
50.116.23.104	147.237.77.234	United States	halag.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
109.64.86.171	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	2
93.158.203.168	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.69.224	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
221.210.200.245	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
198.52.97.85	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
50.116.123.135	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
167.0.109.153	147.237.0.35	Colombia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.53.43.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
106.51.226.59	147.237.72.167	India	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.168	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.103.132	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
58.218.200.137	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
221.210.200.245	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
195.88.208.193	147.237.76.147	Russian Federation	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.135	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
150.242.238.99	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
45.79.103.178	147.237.77.170	United States	maarachot.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
106.51.226.59	147.237.72.167	India	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
104.128.144.131	147.237.76.201	Canada	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
94.102.48.195	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1

09-09-2016-13:04:08 to 09-09-2016-14:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.177.167.180	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	282
8.37.225.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
46.19.85.146	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
87.70.41.135	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
104.20.50.8	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
104.20.50.8	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
104.20.50.8	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
104.20.50.8	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
104.20.50.8	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
104.20.50.8	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
104.20.50.8	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
104.20.50.8	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
46.19.85.146	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
46.19.86.105	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.253.240.210	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
46.116.215.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.183.13.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
87.106.184.160	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	8
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	8
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
5.22.134.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.210	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
31.168.172.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.85.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.211.153	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
109.253.158.59	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.73	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.13.183	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.73	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
217.132.161.237	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
46.210.128.61	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
109.253.240.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
79.183.13.183	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.201	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
27.254.248.13	Thailand	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
79.183.13.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.76.215.176	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
188.120.148.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.53.43.213	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.178	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
193.43.246.250	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	3
185.3.147.69	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

09-09-2016-13:04:08 to 09-09-2016-14:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	64
37.26.147.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
46.19.86.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
185.32.179.129	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	4
46.116.215.173	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.180.103.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.109.113.192	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
84.109.167.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.138.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
88.202.218.240	United Kingdom	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.139.231.164	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.231.164	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
46.19.85.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
89.237.116.25	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
79.179.146.159	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mainqsachar	Block	1
66.249.76.74	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/apple-app-site-association	Block	1
172.242.65.246	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/1/2871.ppt	Block	1
45.79.103.178	United States	147.237.77.170	maarachot.idf.il	Unknown HTTP Request Method 1 in URL	Block	1
77.139.231.164	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	1
46.120.98.216	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
194.72.238.241	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	1
89.237.116.25	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
31.154.81.17	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.93.156	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
176.13.232.223	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
77.139.231.164	France	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	1
50.116.23.104	United States	147.237.77.234	halag.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
194.242.168.16	France	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
109.64.38.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
80.148.27.130	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.93.158	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
185.3.147.254	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
79.177.167.180	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.102.9.6	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
207.46.13.180	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/src="http:/www.youtube.com/v/0mwqtcld1fe	Block	1
109.66.31.71	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
45.79.103.178	United States	147.237.77.170	maarachot.idf.il	Malformed HTTP Header Line 2	Block	1
69.164.205.7	United States	147.237.77.235	sviva.idf.il	Multiple Untraceable SSL Sessions from 69.164.205.7 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
46.19.86.210	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
79.178.194.176	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
109.253.158.59	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
45.79.103.178	United States	147.237.77.170	maarachot.idf.il	Malformed URL	Block	1

09-09-2016-13:04:08 to 09-09-2016-14:04:08