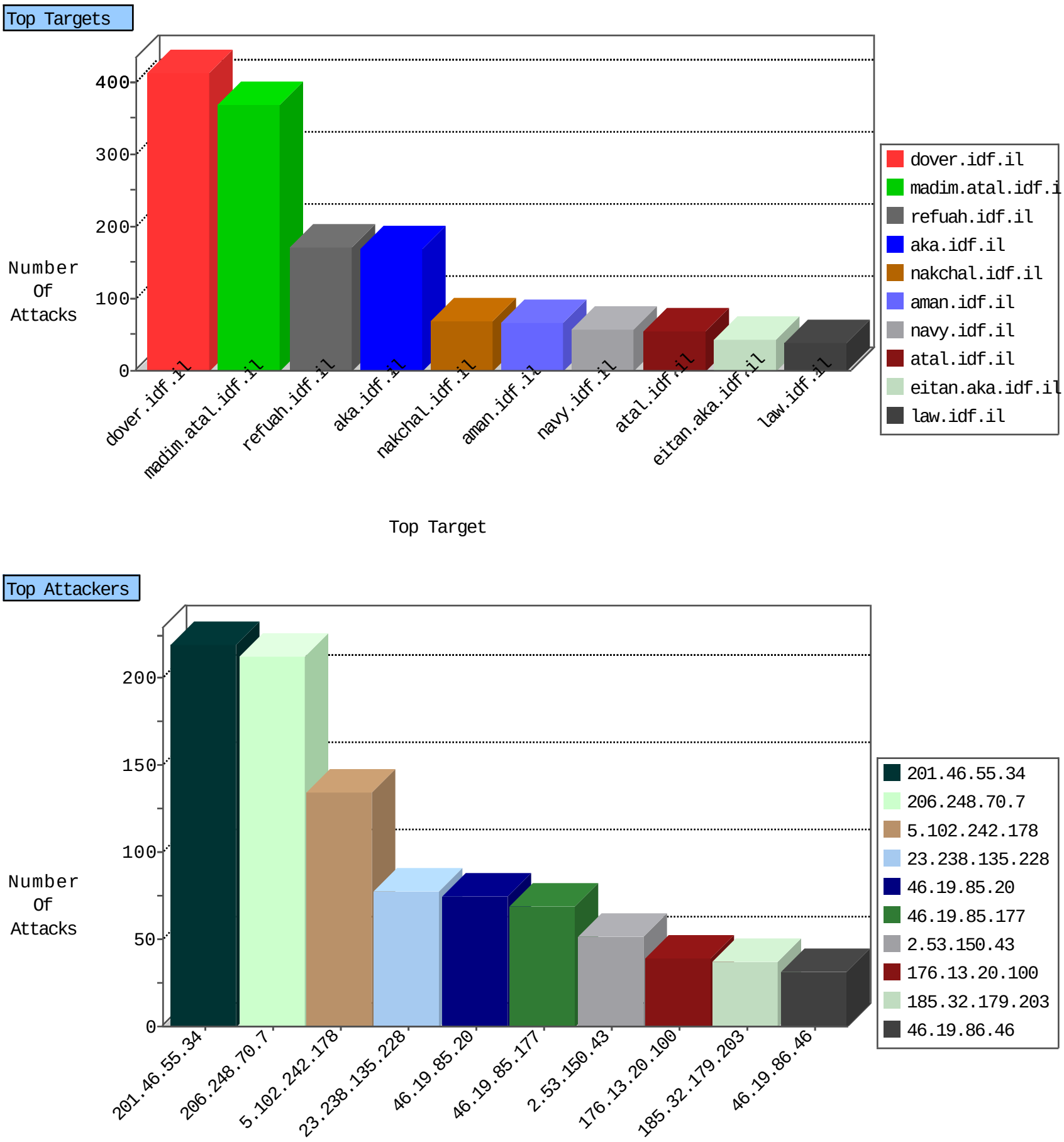
09-08-2016-13:04:03 to 09-08-2016-14:04:03

IDF Under Attack
Daily Report



09-08-2016-13:04:03 to 09-08-2016-14:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	177
46.19.86.143	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
85.64.146.126	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
58.218.200.137	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
71.6.216.47	United States	147.237.76.30	himush.idf.il	Black List	drop	1

09-08-2016-13:04:03 to 09-08-2016-14:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
206.248.70.7	Puerto Rico	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	194
206.248.70.7	Puerto Rico	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	16
77.67.47.7	France	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.46.19	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
51.254.97.218	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
206.248.70.7	Puerto Rico	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	3
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

09-08-2016-13:04:03 to 09-08-2016-14:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
77.67.47.7	147.237.77.74	France	law.idf.il	SQL Injection - Select From	10
184.168.46.19	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	7
185.27.106.90	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	4
79.181.166.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.35.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.13.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.218.200.137	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
197.40.51.85	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
12.139.34.20	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
113.240.250.154	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
12.139.34.20	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
91.121.116.113	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
81.218.55.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.250.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.31.27	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.25.102.63	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.218.200.137	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.93.185.10	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.168.31.135	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
12.139.34.20	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.195	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
2.55.14.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.168.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-08-2016-13:04:03 to 09-08-2016-14:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.85.20	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	37
46.19.85.20	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
201.46.55.34	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
201.46.55.34	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
201.46.55.34	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
201.46.55.34	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
201.46.55.34	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
201.46.55.34	Brazil	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
147.235.236.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
176.13.226.249	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
201.46.55.34	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
201.46.55.34	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	19
195.60.235.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
46.19.86.46	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	14
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.14	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.86.46	Israel	147.237.77.233	atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	11
185.32.179.203	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.85.145	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
62.0.200.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
62.0.200.211	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
185.99.33.8	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.145	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
23.238.135.228	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.86.145	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
23.238.135.228	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
62.0.236.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
23.238.135.228	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
23.238.135.228	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
23.238.135.228	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
23.238.135.228	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.34	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
46.19.85.83	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
23.238.135.228	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
23.238.135.228	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.85.145	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
201.46.55.34	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.96	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.79	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
201.46.55.34	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
201.46.55.34	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
89.218.77.238	Kazakstan	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
185.32.179.203	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
201.46.55.34	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
185.32.179.203	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
201.46.55.34	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
62.0.212.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.55.0.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

09-08-2016-13:04:03 to 09-08-2016-14:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.102.242.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	135
46.19.85.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	69
2.53.150.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	52
176.13.20.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37
176.13.16.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
109.253.241.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
109.253.202.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
147.236.113.1	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	6
5.29.204.71	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	5
37.26.147.159	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
109.253.241.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.158.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.196.233	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	3
109.253.143.38	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
2.55.185.30	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
212.179.28.34	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.185.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.194.0	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.64.22	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.22	Block	2
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	2
109.253.133.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.173	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2090.jpg	Block	1
85.64.240.109	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
46.19.85.11	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.53.12.254	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
193.124.58.72	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
77.124.19.17	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/0/	Block	1
46.19.86.112	Israel	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method g: in URL gzip,	Block	1
157.55.39.115	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/watch	Block	1
46.19.85.96	Israel	147.237.76.42	refuah.idf.il	Multiple Malformed URL from 46.19.85.96	Block	1
80.246.130.159	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
176.13.251.195	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/71545.pdf	Block	1
46.19.85.20	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
85.64.245.112	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
77.138.21.211	France	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.138.21.211	Block	1
46.116.100.211	Israel	147.237.72.166	aka.idf.il	Unknown Parameter y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.85.96	Israel	147.237.76.42	refuah.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.96	Block	1
80.246.139.74	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
185.22.224.96	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	1
66.249.76.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
46.19.85.96	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
87.69.51.60	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/סו''ג	Block	1
213.57.59.50	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.138.21.211	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
66.102.9.3	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
46.19.85.96	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method zvvllq45q1ad0lr2 in URL	Block	1
82.80.193.240	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
185.120.125.29	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1

09-08-2016-13:04:03 to 09-08-2016-14:04:03