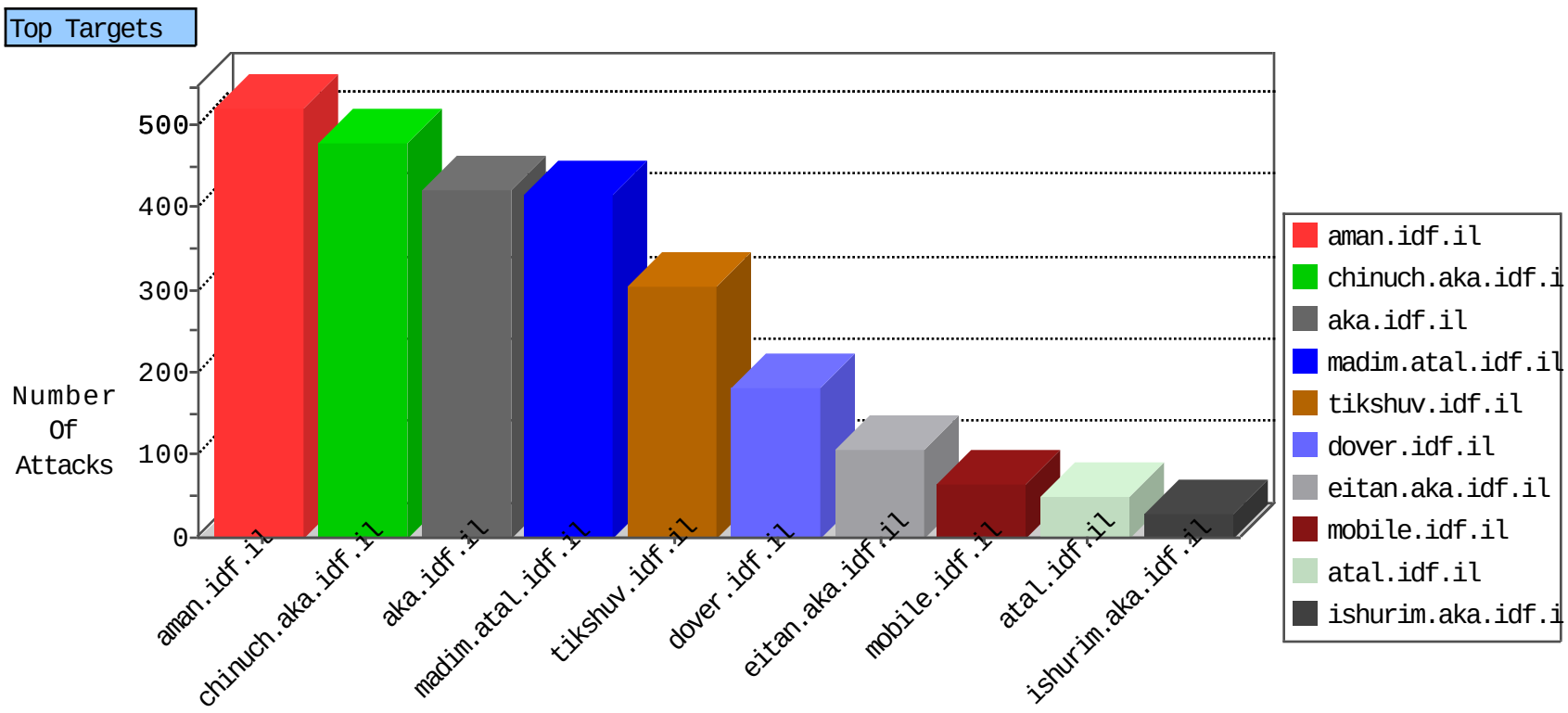
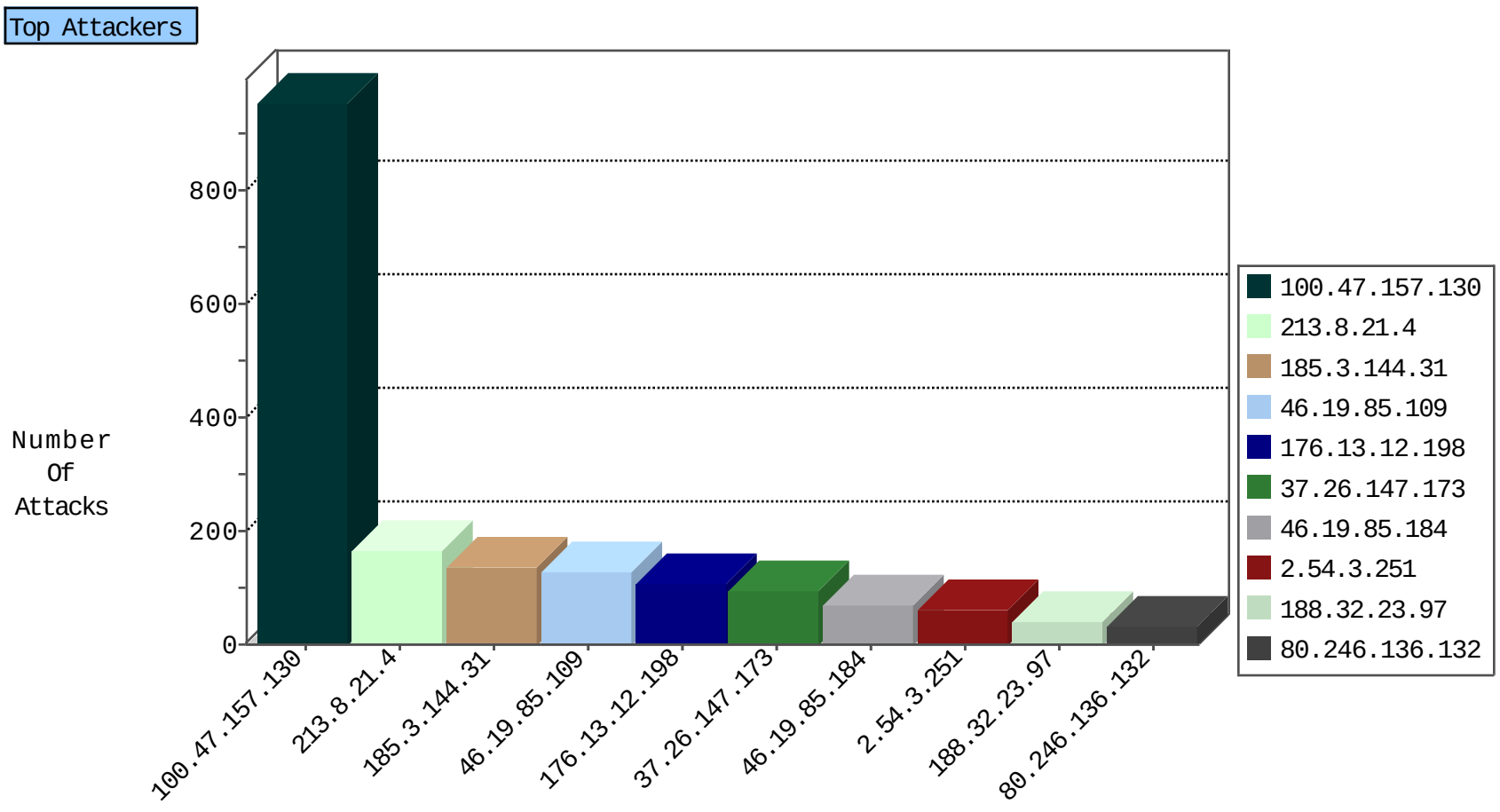
02-10-2016-15:04:05 to 02-10-2016-16:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-10-2016-15:04:05 to 02-10-2016-16:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.7	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
115.239.228.10	China	147.237.76.176	test.ncore.idf.il	JLM_Purple_Con_Limit_Http	drop	3
115.239.228.10	China	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Http	drop	2
142.54.169.163	United States	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
142.54.160.210	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1

02-10-2016-15:04:05 to 02-10-2016-16:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
187.38.150.123	Brazil	147.237.77.216	dover.idf.i	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

02-10-2016-15:04:05 to 02-10-2016-16:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
192.118.73.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
37.142.68.83	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.153.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.66.15	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.165	147.237.76.176		test.ncore.idf.il	ET SCAN Potential SSH Scan	1
89.139.163.143	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.206.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.242.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.158.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
40.122.132.28	147.237.76.31	United States	nakchal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
31.210.188.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.38.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.161	147.237.0.15		kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
84.109.107.132	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.2.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.116.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.62.153	147.237.72.156	Israel	aman.idf.il	portscan: TCP Distributed Portscan	1

02-10-2016-15:04:05 to 02-10-2016-16:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
100.47.157.130	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	479
100.47.157.130	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	477
176.13.12.198	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
188.32.23.97	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
81.218.147.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.177.29.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.9.111	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.65.11.234	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
2.54.37.203	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
80.246.136.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
77.127.174.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.147.173	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	9
185.32.179.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.64.17.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.98.55.67	Ukraine	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.0.247.129	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.90.132.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
37.26.148.238	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
82.166.112.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.206	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.219.134.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.147.173	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		alert	6
80.74.121.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.147	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.49.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.148.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.237	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.11.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.246.136.132	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
79.179.55.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.152.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.242.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	5
80.246.136.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
108.212.84.251	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
80.246.136.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	5
79.180.161.94	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
80.246.136.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.149.246	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence		monitor	4
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
189.218.208.202	Mexico	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4

02-10-2016-15:04:05 to 02-10-2016-16:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.21.4	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 213.8.21.4	Block	165
185.3.144.31	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	134
46.19.85.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
37.26.147.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
46.19.85.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
2.54.3.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
46.19.85.109	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.109	Block	32
109.253.196.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
46.19.86.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
176.13.2.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
37.26.147.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
46.19.85.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.34.167	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
212.117.151.42	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	5
85.65.77.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	5
46.19.86.189	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	4
85.250.92.56	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.250.92.56	Block	4
84.110.83.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.179.115.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.13.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.143.232.34	Russian Federation	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 188.143.232.34	Block	2
60.50.209.70	Malaysia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
60.50.209.70	Malaysia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	2
188.143.232.40	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 188.143.232.40	Block	2
93.172.244.70	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
46.98.55.67	Ukraine	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
31.168.27.48	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
104.131.69.104	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.63	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/news/<a href=	Block	1
5.29.254.39	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
79.179.49.84	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
69.195.124.96	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/wp-login.php	Block	1
157.55.39.28	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/page.asp	Block	1
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	1
85.250.92.56	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
79.182.56.191	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$6 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
189.218.208.202	Mexico	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
176.13.12.158	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
73.136.215.236	United States	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
109.65.11.234	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.85.109	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
85.64.86.22	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
5.102.220.199	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
188.143.232.34	Russian Federation	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/926-he/	Block	1
69.195.124.96	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 69.195.124.96	Block	1
157.55.39.90	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
85.250.213.249	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/resource/userfollowresource/create/	Block	1

02-10-2016-15:04:05 to 02-10-2016-16:04:05