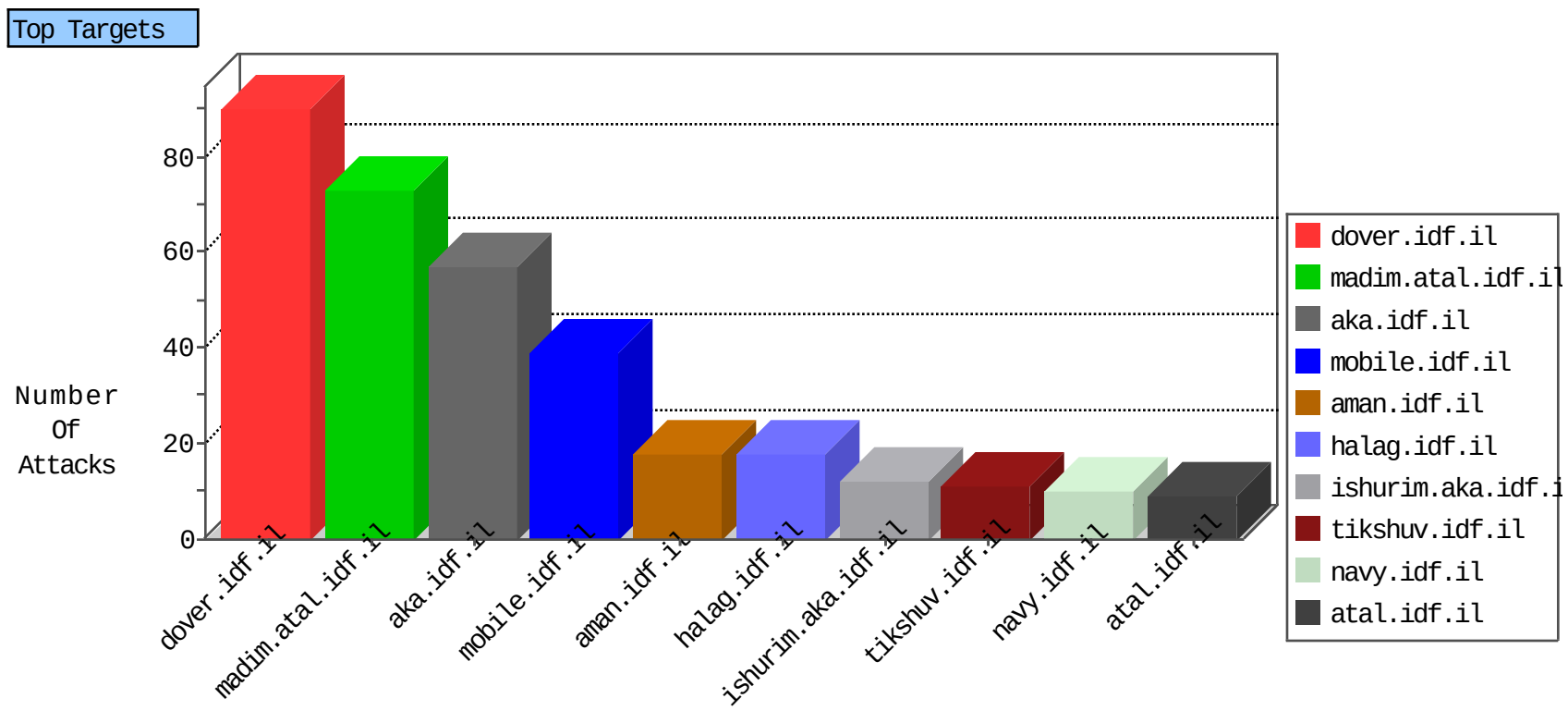
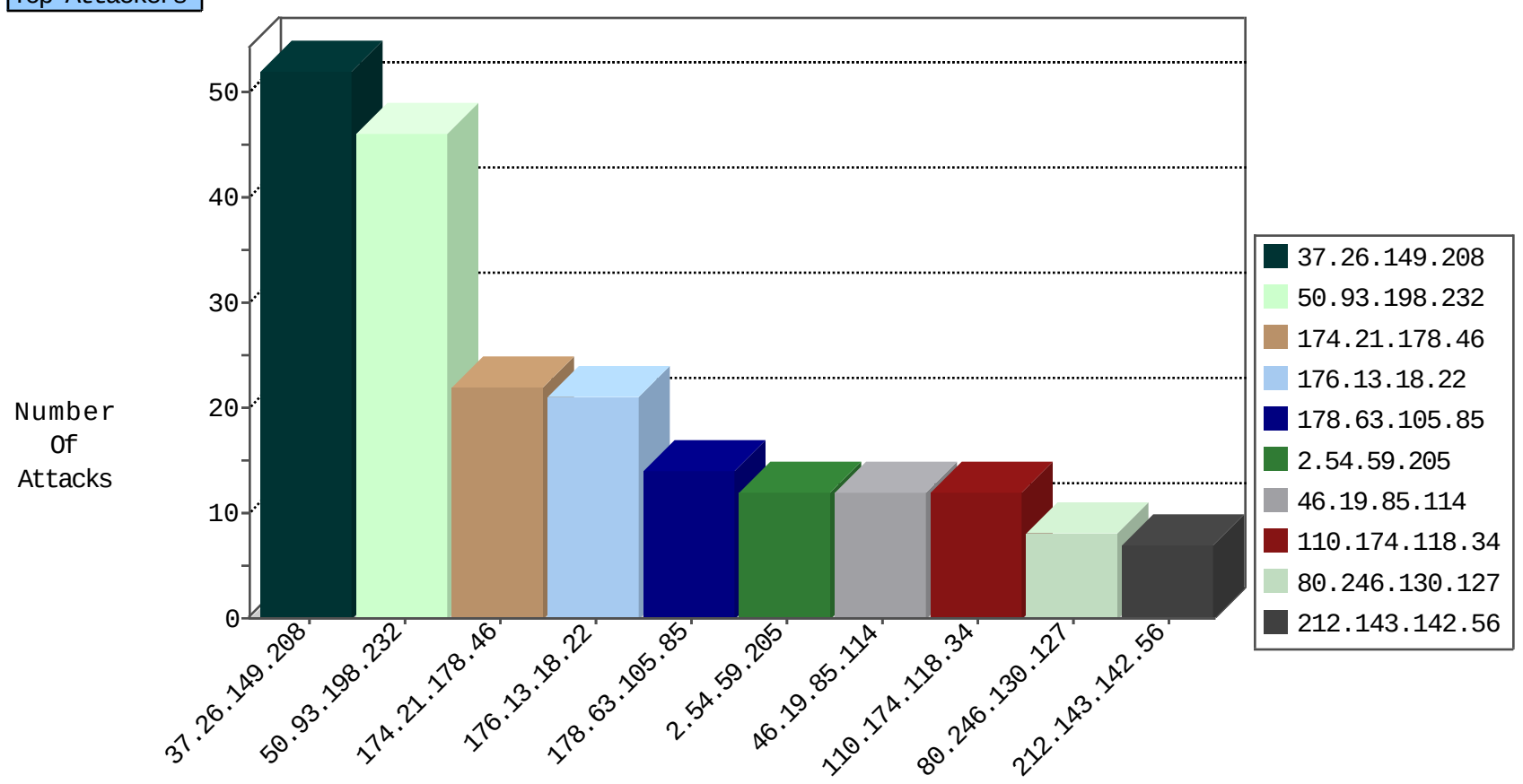
03-07-2016-07:04:07 to 03-07-2016-08:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-07-2016-07:04:07 to 03-07-2016-08:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.103.252.5		147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	4
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
185.56.28.67	Netherlands	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
185.56.28.67	Netherlands	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
105.158.64.104	Morocco	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
105.158.64.104	Morocco	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
185.56.28.67	Netherlands	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1

03-07-2016-07:04:07 to 03-07-2016-08:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
136.243.103.157	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
203.98.92.225	Australia	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-07-2016-07:04:07 to 03-07-2016-08:04:07

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	4
218.246.0.97	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
118.112.185.236	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
118.112.185.236	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
118.112.185.236	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
23.96.109.87	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
218.246.0.97	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.68	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1
118.112.185.236	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
118.112.185.236	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
118.112.185.236	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.76.39		mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1

03-07-2016-07:04:07 to 03-07-2016-08:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
174.21.178.46	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
176.13.18.22	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
110.174.118.34	Australia	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.59.205	Israel	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	7
80.246.130.127	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.85.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.110.53.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.178.28.92	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	4
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	4
79.177.30.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
37.26.149.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.137.90	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.178.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.217.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.47	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.168.218.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.232	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	2
37.19.119.160	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
94.159.168.134	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.8.204.50	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.86.141	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
199.203.215.1	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
80.178.201.2	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.19.119.160	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
84.108.42.204	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.3.144.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.88.41.19	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.64.146.246	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.108	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
176.13.19.237	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.195.172	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.120	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.32.179.144	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
159.226.95.66	China	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.22.130.225	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
80.246.136.208	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.110	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
65.181.113.88	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

03-07-2016-07:04:07 to 03-07-2016-08:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
5.22.130.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
80.246.136.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	4
109.253.208.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
50.93.198.232	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 50.93.198.232	Block	3
2.52.21.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
50.93.198.232	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
2.54.59.205	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	2
109.253.207.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
50.93.198.232	United States	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	2
50.93.198.232	United States	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	2
50.93.198.232	United States	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	2
50.93.198.232	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 50.93.198.232	Block	2
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
50.93.198.232	United States	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 50.93.198.232	Block	2
50.93.198.232	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 50.93.198.232	Block	2
50.93.198.232	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
50.93.198.232	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
50.93.198.232	United States	147.237.0.15	kosher-kravi.idf.il	Distributed PHP Attempt	Block	2
50.93.198.232	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 50.93.198.232	Block	2
37.19.119.160	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
50.93.198.232	United States	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	2
50.93.198.232	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	2
50.93.198.232	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 50.93.198.232	Block	2
50.93.198.232	United States	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	2
50.93.198.232	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
50.93.198.232	United States	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 50.93.198.232	Block	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
50.93.198.232	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/xmlrpc.php	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	1
50.93.198.232	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
50.93.198.232	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/xmlrpc.php	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
66.249.64.230	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
46.229.164.98	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
50.93.198.232	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 50.93.198.232	Block	1
79.178.28.92	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
40.77.167.61	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
199.116.171.53	United States	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
50.93.198.232	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 50.93.198.232	Block	1
50.93.198.232	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 50.93.198.232	Block	1
97.91.157.117	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.229.164.98	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
50.93.198.232	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
117.241.138.33	India	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.155.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
40.77.167.75	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.64.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
212.150.209.205	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58628	Block	1

03-07-2016-07:04:07 to 03-07-2016-08:04:07