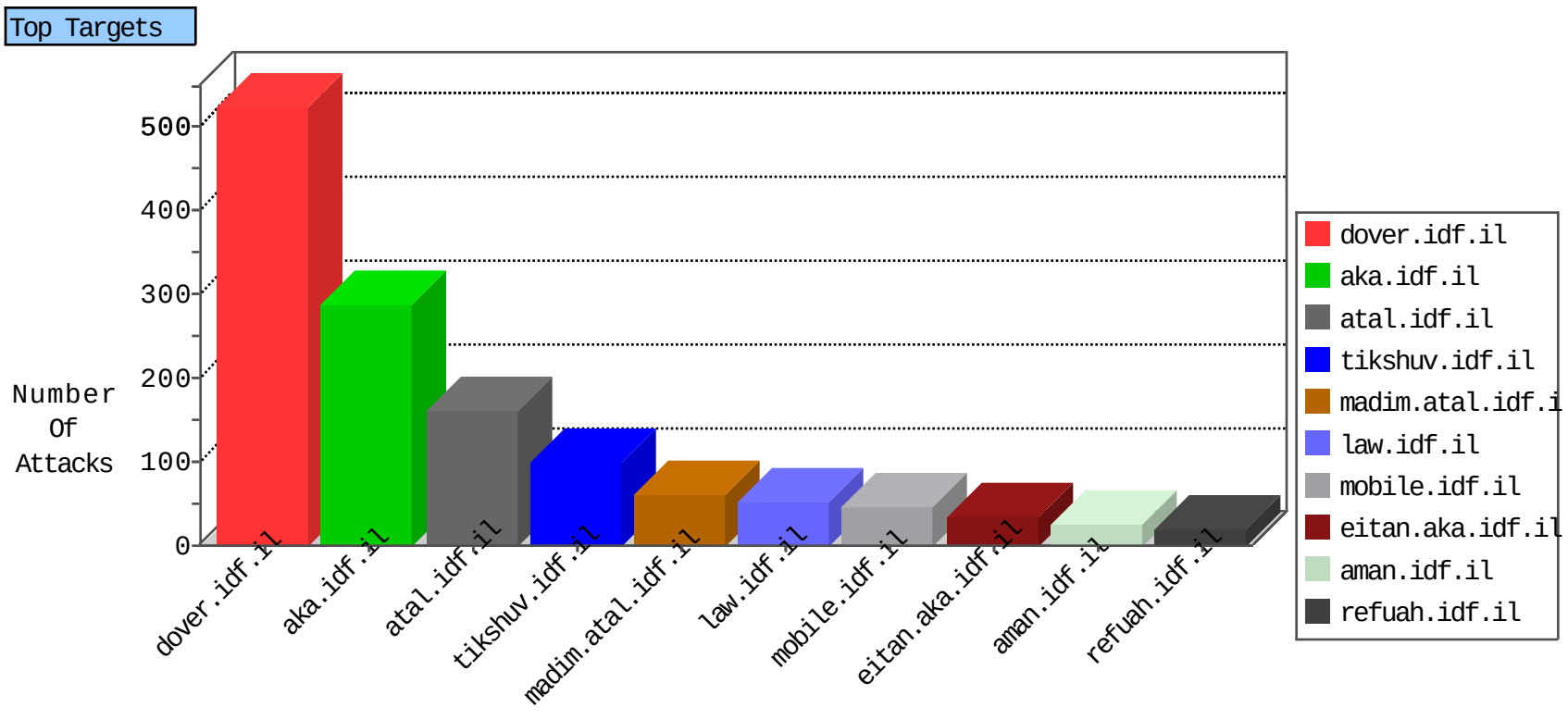
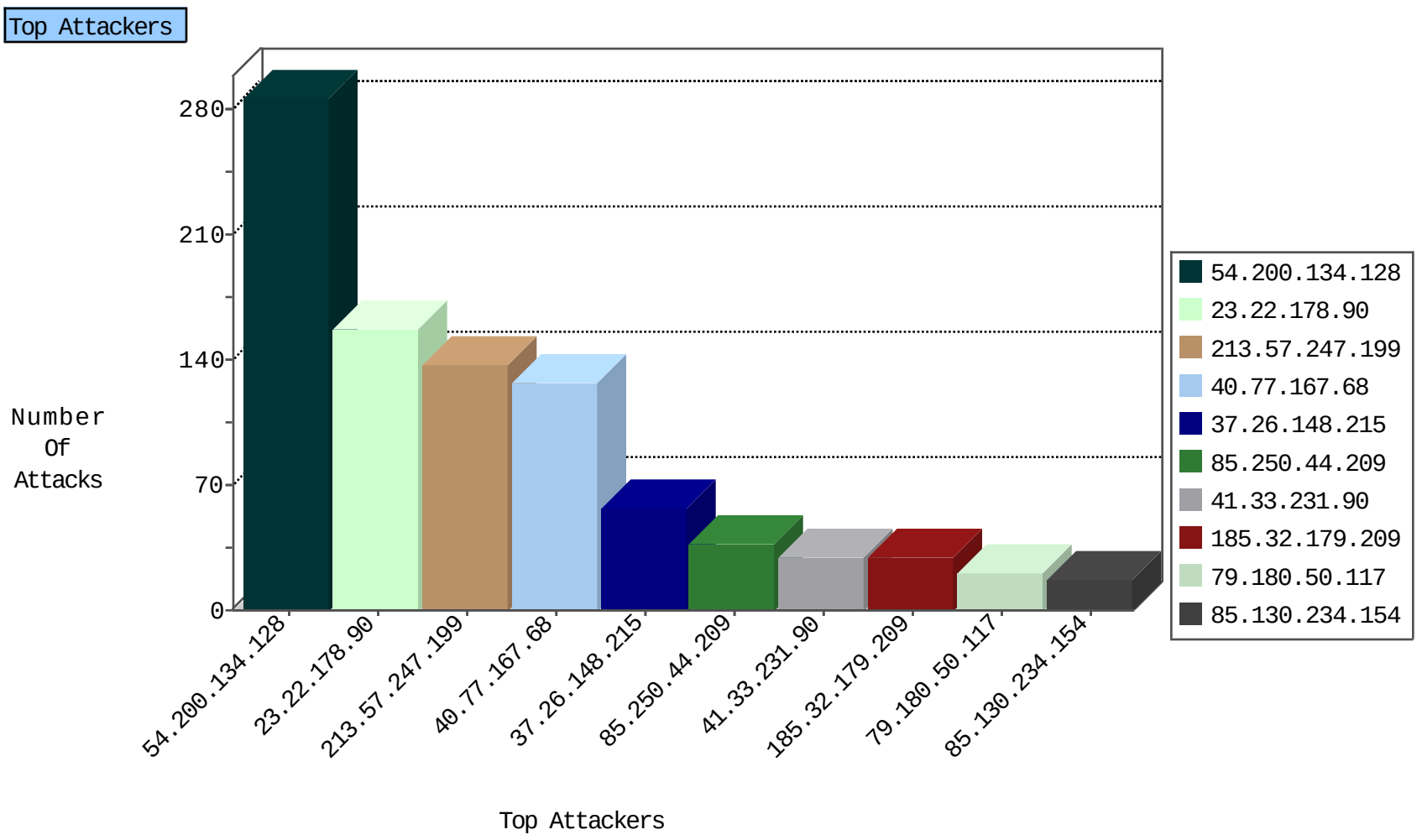
02-12-2016-15:04:04 to 02-12-2016-16:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-12-2016-15:04:04 to 02-12-2016-16:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
54.200.134.128	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
89.248.160.138	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
89.248.174.4	Netherlands	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
170.161.102.40	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

02-12-2016-15:04:04 to 02-12-2016-16:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.127.236.87	Israel	147.237.77.170	maarachot.idf.il	C122: HTTP: Access to - .exe or .dll	Permit	1
91.121.221.15	France	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

02-12-2016-15:04:04 to 02-12-2016-16:04:04

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
185.130.5.102	147.237.77.176		matpash.idf.il	ET SCAN NMAP -sS window 1024	1
113.93.49.137	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
74.122.192.101	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
74.122.192.101	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
40.114.47.160	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
201.235.215.254	147.237.8.46	Argentina	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
201.235.215.254	147.237.8.46	Argentina	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
193.105.134.220	147.237.0.34	Sweden	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
74.122.192.101	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
74.122.192.101	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
46.45.137.67	147.237.0.16	Turkey	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
212.158.148.91	147.237.76.30	Czech Republic	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
201.235.215.254	147.237.8.46	Argentina	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1

02-12-2016-15:04:04 to 02-12-2016-16:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.200.134.128	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	228
213.57.247.199	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	138
40.77.167.68	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	126
23.22.178.90	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	122
54.200.134.128	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	57
37.26.148.215	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
23.22.178.90	United States	147.237.76.200	eitan.aka.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
46.19.86.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.182.189.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.207.73	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.157.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.193	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.140.59.136	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.234		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
2.54.164.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
85.130.234.154	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.120.72.173	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.172.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.72.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.234.154	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.32	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.244	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.130.234.154	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.244	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.148.215	Israel	147.237.0.34	tikshuv.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.86.32	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.121.72.249	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
149.88.20.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.228.159.63	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.108.4.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
2.54.132.88	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
173.252.105.115	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
66.249.65.122	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
185.89.217.230		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
212.116.162.6	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
185.89.217.228		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
23.22.178.90	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
84.108.4.27	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.22.135.177	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.3.147.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.126.20.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.229.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.215	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3

02-12-2016-15:04:04 to 02-12-2016-16:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.250.44.209	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 85.250.44.209	Block	37
185.32.179.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
79.180.50.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
23.22.178.90	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 23.22.178.90	Block	5
66.249.65.14	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.65.14	Block	4
87.69.87.196	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	4
176.13.13.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.154.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	3
176.13.18.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
94.65.134.134	Greece	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	1
37.26.148.193	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.26.148.193	Block	1
5.28.135.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$116 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
185.89.217.224		147.237.77.74	law.idf.il	URL is Above Root Directory www.law.idf.il/../images/1.he/navigation/navigation_arrow.gif	Block	1
66.249.78.20	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
46.120.178.174	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 46.120.178.174	Block	1
136.243.67.234	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
84.108.204.229	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
23.22.178.90	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter l in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
77.127.236.87	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 77.127.236.87	Block	1
213.8.204.66	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
94.65.134.134	Greece	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/xmlrpc.php	Block	1
37.26.148.193	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	1
5.28.135.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$45 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
79.180.99.151	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.78.27	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1073-he/nakhal.aspx	Block	1
193.201.227.106	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.121.73.84	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
149.78.224.98	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
84.228.132.221	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
23.22.178.90	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
77.127.236.87	Israel	147.237.77.170	maarachot.idf.il	Multiple _vti_ from 77.127.236.87	Block	1
213.8.204.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
41.191.45.250	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
109.253.207.73	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.102.216.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
80.178.124.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.78.239	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/news/news.in.aspx	Block	1
193.201.227.106	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
46.121.204.143	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
149.78.239.208	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
31.168.157.182	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.229.1.167	Italy	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
77.127.236.87	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/_vti_bin/owssvr.dll	Block	1
176.228.159.63	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
41.191.45.250	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
118.173.222.226	Thailand	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.108.4.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.245	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/opcemetery/opcemetery.aspx	Block	1

02-12-2016-15:04:04 to 02-12-2016-16:04:04