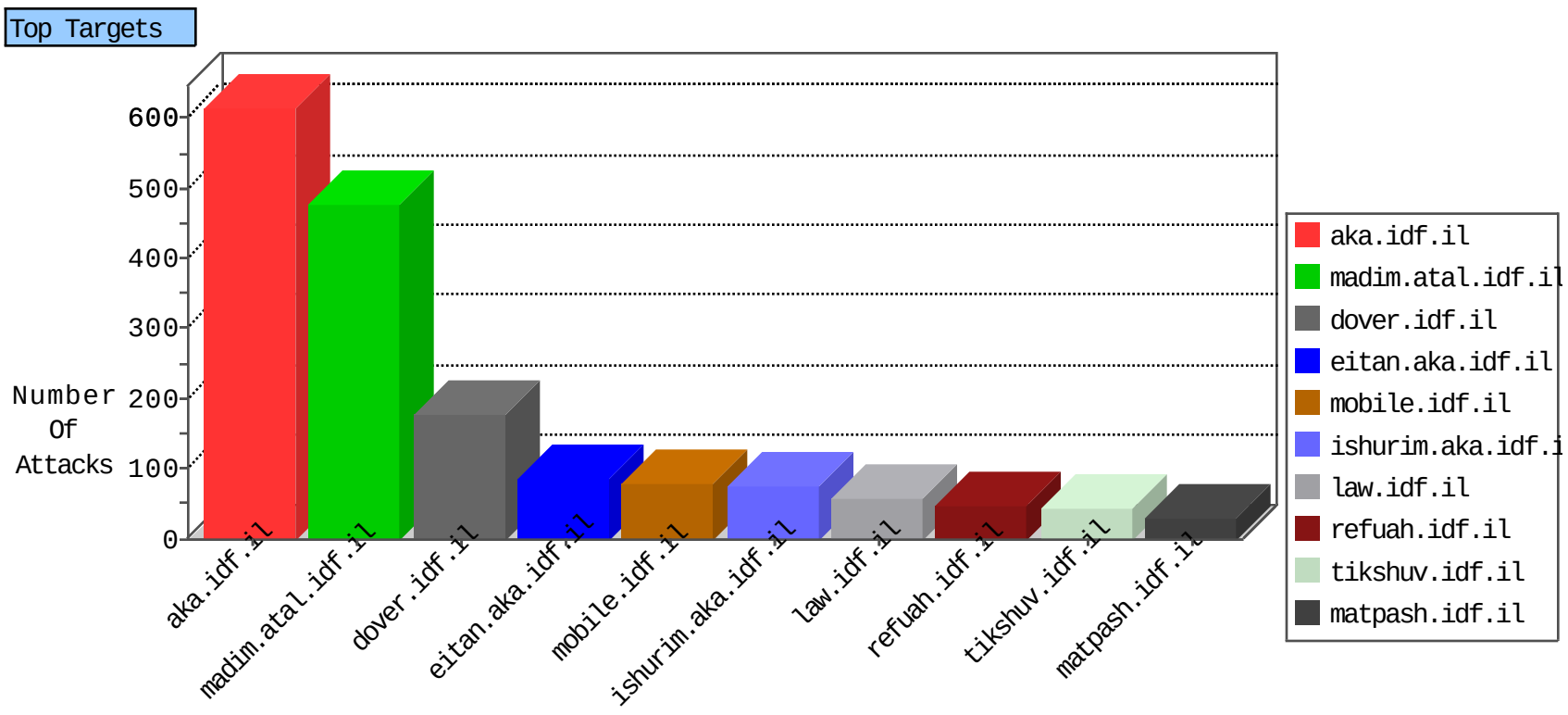
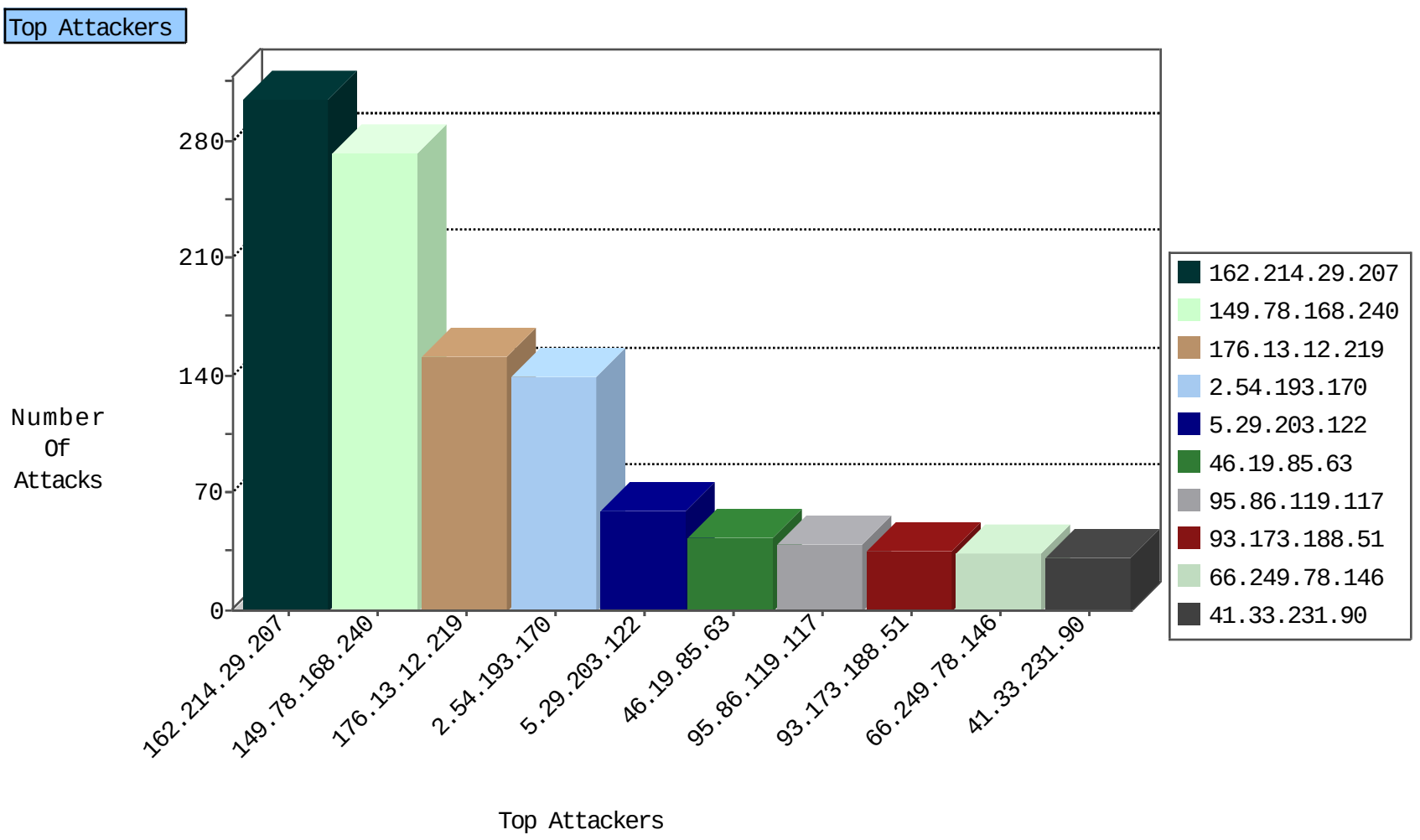
02-27-2016-23:04:05 to 02-28-2016-00:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-27-2016-23:04:05 to 02-28-2016-00:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.209.16	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	12
168.235.207.43	United States	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Http	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
134.147.203.115	Germany	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
168.235.207.43	United States	147.237.77.233	atal.idf.il	JLM_Under_Attack_Con_Http	drop	1
77.81.191.126	Romania	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
95.15.14.194	Turkey	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
52.28.32.164	United States	147.237.76.202	e.halag.idf.il	JLM_Purple_Con_Limit_Https	drop	1
193.182.144.142	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
205.209.185.11	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
95.15.14.194	Turkey	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
71.6.158.166	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
205.209.185.11	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
95.15.14.194	Turkey	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

02-27-2016-23:04:05 to 02-28-2016-00:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.133.255	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
162.214.29.207	United States	147.237.72.166	aka.idf.il	22095: HTTP: Joomla Image Manager folderRename Security Bypass Vulnerability	Block	11
162.214.29.207	United States	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	11
46.19.85.40	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
84.108.154.41	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
61.135.189.121	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
109.67.149.87	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
84.94.41.65	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

02-27-2016-23:04:05 to 02-28-2016-00:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.214.29.207	147.237.72.166	United States	aka.idf.il	Tehila - Perl LWP with fake user agent	76
162.214.29.207	147.237.72.166	United States	aka.idf.il	SERVER-WEBAPP Mambo upload.php access	40
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
89.248.162.167	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
62.210.69.71	147.237.76.30	France	himush.idf.il	ET SCAN Potential SSH Scan	1
45.63.97.54	147.237.76.202		e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.97.54	147.237.0.33		idf.il	ET SCAN NMAP -sS window 1024	1
196.203.83.25	147.237.8.45	Tunisia	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
190.69.234.105	147.237.76.30	Colombia	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.248.162.167	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1
89.248.162.167	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
45.63.97.54	147.237.77.234		halag.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.97.54	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.97.54	147.237.0.15		kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.162.167	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1

02-27-2016-23:04:05 to 02-28-2016-00:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.193.170	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	63
5.29.203.122	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
2.54.193.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	41
95.86.119.117	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.54.193.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	35
212.76.124.189	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
77.127.211.169	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.253.131.239	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
195.154.173.103	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
168.235.207.43	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
84.110.144.86	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
46.19.86.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.71	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
79.182.109.10	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
79.180.105.20	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	8
89.139.159.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
62.0.118.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.172.147.78	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.223	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
120.52.72.42	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
79.179.4.252	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
37.142.68.28	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
190.98.49.30	Suriname	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence		monitor	4
85.250.177.205	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.254.113	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.71	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
185.3.144.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.55.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.55.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.174	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
195.154.173.103	France	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
109.66.28.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.16	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
149.78.171.41	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
109.253.156.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.88.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-27-2016-23:04:05 to 02-28-2016-00:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.168.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	273
176.13.12.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	151
162.214.29.207	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	75
162.214.29.207	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 162.214.29.207	Block	73
93.173.188.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
162.214.29.207	United States	147.237.72.166	aka.idf.il	Multiple signatures from 162.214.29.207	Block	18
66.249.78.146	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	13
176.13.5.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
66.249.79.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	5
79.179.4.252	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	5
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	4
94.159.146.64	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
178.137.81.41	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	3
109.253.215.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.247.56	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.29.247.56	Block	2
213.57.221.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.111.210.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.216.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
95.86.119.117	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 95.86.119.117	Block	2
89.139.159.250	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
131.253.25.130	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
188.163.70.39	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1561-en/dover.aspx'	Block	2
93.173.187.237	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.5.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/main/home/default.aspx	Block	1
141.212.122.225	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
66.249.64.185	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
95.86.108.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/&sa=u&ved=0ahukewjk4y2r7pjlahubobqkhr_raxwqfggimaa&usg=afqjcngtytnlljmpnyfpfndzekjk-ayw9g	Block	1
46.19.85.63	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
79.179.4.252	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
146.185.234.48	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.29.247.56	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/site/spotting/spotting.asp	Block	1
85.65.137.86	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter Do.. in www.aka.idf.il/giyus/general/default.asp	None	1
46.116.222.104	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$7 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
113.76.90.154	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter Do.. in www.aka.idf.il/giyus/kadatz/	None	1
24.154.4.247	United States	147.237.76.31	nakchal.idf.il	Abnormally Long Request method	Block	1
95.86.119.117	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sip_storage	Block	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter doc.. in www.aka.idf.il/giyus/forms/	None	1
162.214.29.207	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/index.php	Block	1
46.120.48.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
95.86.104.100	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/sip_storage/files/7/1437.pdf/	Block	1
79.180.35.186	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
157.55.39.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.33	United States	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
24.154.4.247	United States	147.237.76.31	nakchal.idf.il	Illegal Byte Code Character in Method	Block	1
109.66.55.33	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
93.172.147.78	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/faq.aspx	None	1
138.36.0.3		147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/index.php	Block	1

02-27-2016-23:04:05 to 02-28-2016-00:04:05