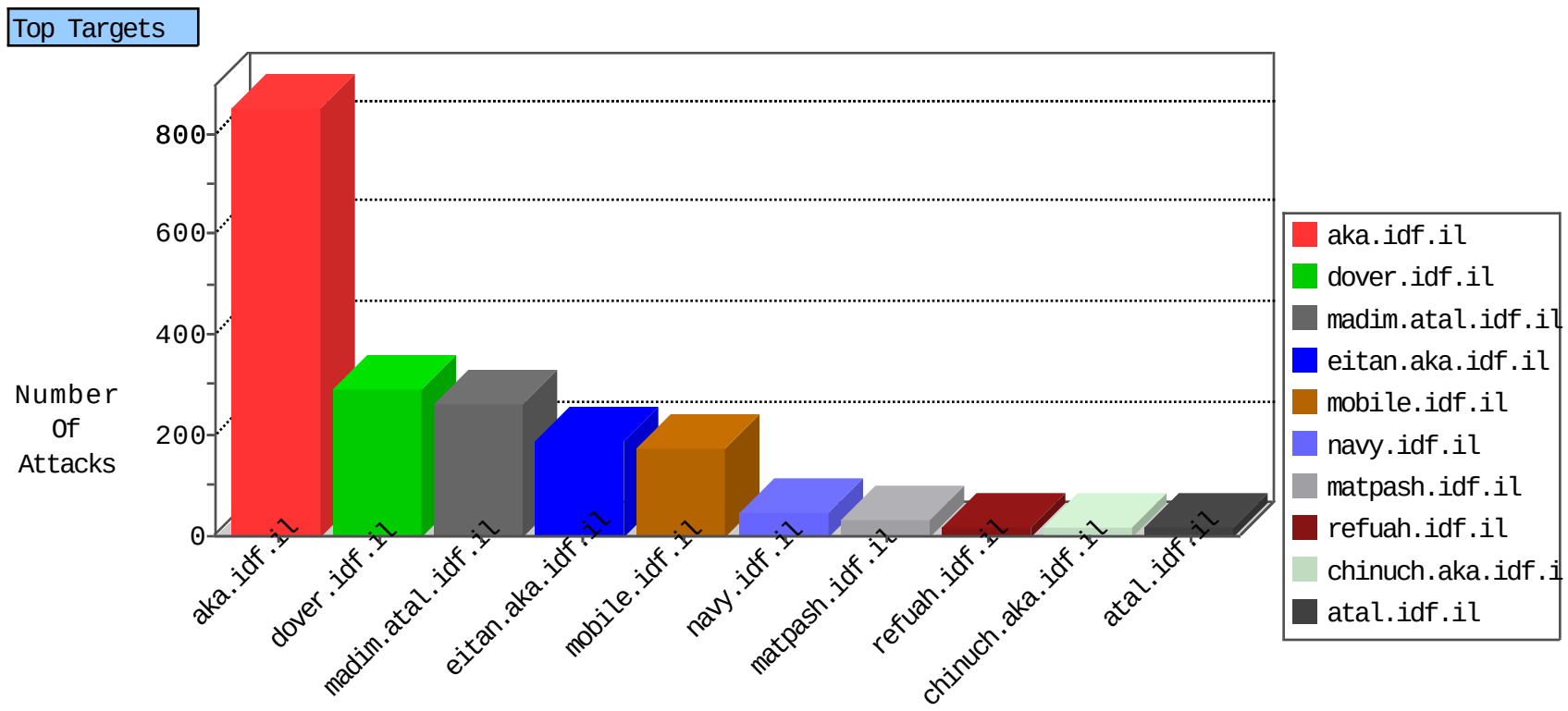
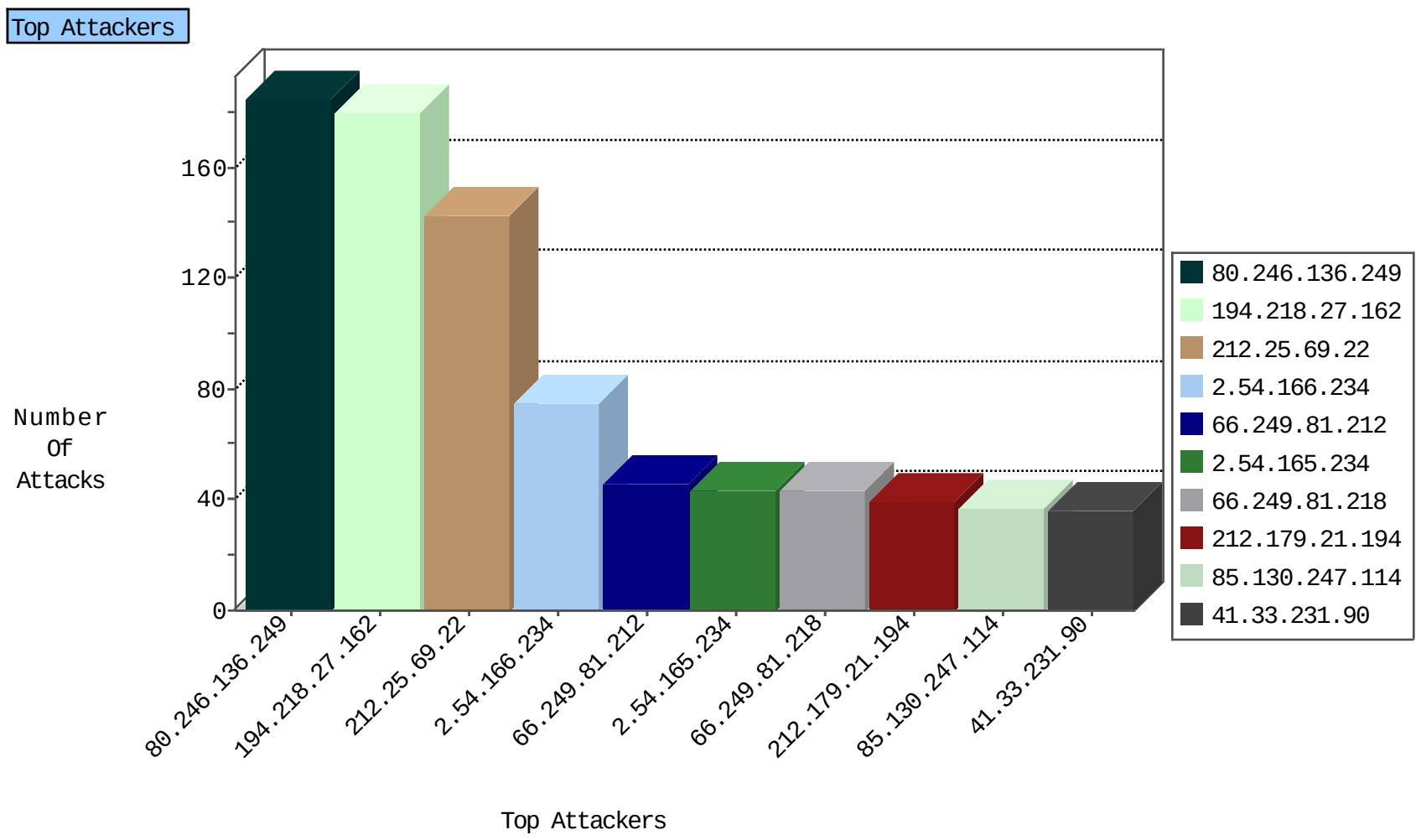
02-29-2016-21:04:03 to 02-29-2016-22:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-29-2016-21:04:03 to 02-29-2016-22:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.123.192	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	21
79.180.123.192	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	14
82.145.218.250	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	2
185.94.111.1		147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
91.121.183.16	France	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
37.26.148.239	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1		147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
91.121.183.16	France	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
42.112.10.75	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
185.35.62.148	Switzerland	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
42.112.10.81	Vietnam	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
91.121.183.16	France	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
23.239.64.15	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1

02-29-2016-21:04:03 to 02-29-2016-22:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.110	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
69.30.201.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.203.166	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
94.159.169.172	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
123.126.68.116	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

02-29-2016-21:04:03 to 02-29-2016-22:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.69.26	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	10
80.246.136.249	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.81	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
2.52.140.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
193.105.134.220	147.237.0.35	Sweden	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
5.104.111.218	147.237.77.212	Germany	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
178.60.158.173	147.237.0.33	Spain	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.104.111.218	147.237.77.212	Germany	e.dover.idf.il	ET SCAN NMAP -f -sS	1
125.227.64.115	147.237.0.200	Taiwan	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.62.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.49.151	147.237.0.33	Netherlands	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.108.165.229	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
68.180.228.112	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
203.197.205.118	147.237.72.14	India	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
66.249.66.149	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
193.105.134.220	147.237.77.226	Sweden	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.121.253.199	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
187.44.109.33	147.237.76.34	Brazil	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.104.111.218	147.237.77.212	Germany	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
149.88.205.102	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.186.143.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.49.151	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.193	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
203.197.205.118	147.237.72.14	India	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1

02-29-2016-21:04:03 to 02-29-2016-22:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
212.25.69.22	Israel	147.237.76.200	eitan.aka.idf.il	drop	First packet isn't SYN	drop	93
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
212.25.69.22	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
85.130.247.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
2.54.166.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	31
37.26.147.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.253.139.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.253.132.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	14
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	13
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
79.177.98.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.179.15.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.137.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.13.29	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.208.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.166.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
2.54.166.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.54.166.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
2.54.166.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
94.230.86.17	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
37.189.210.138	Portugal	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
2.54.166.13	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
41.33.145.214	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.53	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.205.66	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
82.80.131.234	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
213.244.119.251	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
2.54.155.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.60.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.10.41.114	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.86.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.194.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.29.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.159.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.5.79	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.116.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
199.30.24.53	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.119.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.125.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

02-29-2016-21:04:03 to 02-29-2016-22:04:03

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
41.33.145.214	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.246.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.37.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

02-29-2016-21:04:03 to 02-29-2016-22:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	180
2.54.165.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
31.210.188.110	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.210.188.110	Block	13
46.19.86.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
31.210.188.110	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	7
84.108.146.196	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.146.196	Block	5
109.253.132.182	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
37.26.147.245	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.139.152	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.13.13.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.226.21.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
79.182.203.93	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.182.203.93	Block	3
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	3
84.108.146.196	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
46.19.86.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.182.53.14	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
62.219.140.228	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.0.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.182.172.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
209.88.157.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.140.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.180.14.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.13.29	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	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
79.177.98.172	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 79.177.98.172 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
109.65.242.205	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.120.182.19	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	2
79.176.228.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.137.91	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
85.65.120.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.138.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.66.196.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.131.84	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 2.54.131.84	Block	2
82.163.68.250	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	2
109.186.153.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.148.174	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.182.203.93	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
37.26.146.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.96	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;pageNum in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
97.74.215.78	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
87.71.10.143	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
79.177.98.172	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name •ê[[#31]]ŠÆ=¬•[[#5]]}"Ú>[[#29]]nN°ð¾d[[#29]]þ*¾¸[[#24]]\[[#2]](•žÖ^Œ «JTXc"³¹©iq¤e.è°þ•[[#14]]©[[#0]][[#31]]T³ðr[[#14]]»²[[#22]]dÞo&¢øQ*š"µÇ[[#21]]ÇE¬q†	Block	1
66.249.66.96	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/yohalan/main/main.asp	None	1
46.117.229.253	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
84.94.171.214	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.66.96	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;sidescroll in www.aka.idf.il/giyus/kadatz/	None	1
37.189.210.138	Portugal	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.66.96	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/chinuch/klali/default.asp	None	1
89.138.170.91	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
5.9.43.242	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1

02-29-2016-21:04:03 to 02-29-2016-22:04:03