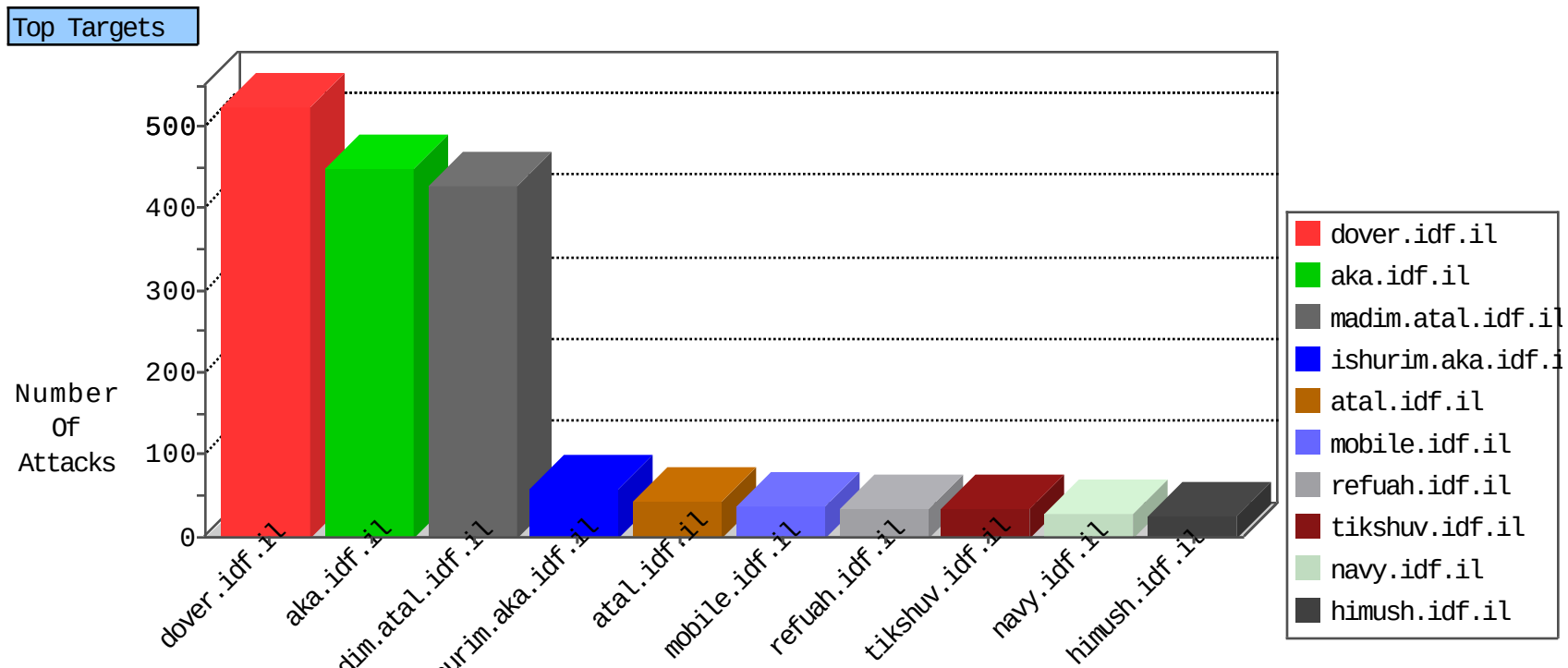
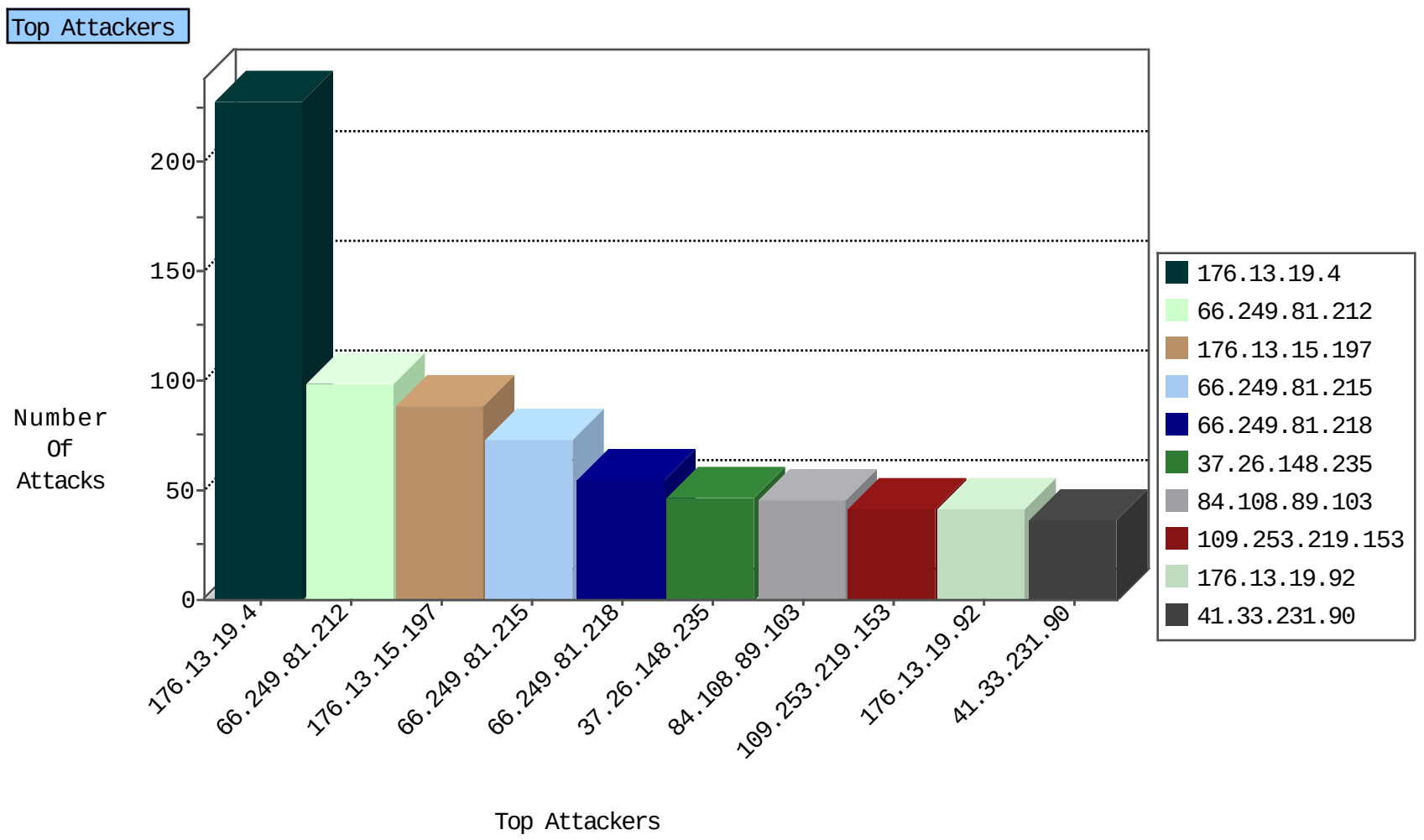
02-04-2016-17:04:01 to 02-04-2016-18:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-04-2016-17:04:01 to 02-04-2016-18:04:01

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	drop	10
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
66.249.81.212	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
208.67.1.60	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

02-04-2016-17:04:01 to 02-04-2016-18:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.254.202.163	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

02-04-2016-17:04:01 to 02-04-2016-18:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.197.121.148	147.237.77.176	United Kingdom	matpash.idf.il	ET SCAN NMAP -sA (2)	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
37.26.146.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.37.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.220.48.217	147.237.8.50	Iran, Islamic Republic of	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
212.143.41.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.85.35.211	147.237.76.197	Bulgaria	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
5.220.48.217	147.237.8.50	Iran, Islamic Republic of	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
185.32.179.119	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.85.35.211	147.237.76.197	Bulgaria	e.himush.idf.il	ET SCAN NMAP -f -sS	1
62.219.13.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.114	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
46.148.22.26	147.237.77.74	Lithuania	law.idf.il	ET SCAN Potential SSH Scan	1
87.68.43.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.148.22.26	147.237.72.14	Lithuania	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
85.64.218.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.214	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.38.42	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.81.10.126	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.105.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.220.48.217	147.237.8.50	Iran, Islamic Republic of	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
77.85.35.211	147.237.76.197	Bulgaria	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
176.13.21.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.81.206	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
93.173.239.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.148.22.26	147.237.77.234	Lithuania	halag.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.76.201	Ukraine	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.148.22.26	147.237.72.217	Lithuania	e.idf.il	ET SCAN Potential SSH Scan	1
87.64.100.21	147.237.77.216	Belgium	dover.idf.il	portscan: TCP Distributed Portscan	1
46.148.22.26	147.237.8.46	Lithuania	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
84.111.240.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.53	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.18.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-04-2016-17:04:01 to 02-04-2016-18:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
176.13.19.92	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	21
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
2.52.39.203	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	17
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
109.253.220.114	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
84.108.89.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	14
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
100.3.95.112	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	13
109.253.220.114	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.88.180.54	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.150.178.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	12
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
31.210.187.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
87.69.67.89	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
84.108.89.103	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
109.65.154.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.148.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.148.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
176.13.21.77	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.118.36.53	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
176.13.15.197	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.118.36.53	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.21.77	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
168.63.137.102	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
84.108.89.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
84.108.89.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	7
84.108.89.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.253.147.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.202.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.150.178.127	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
192.118.36.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.235	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
149.78.42.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.235	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.244.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.151.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.19.92	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	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

02-04-2016-17:04:01 to 02-04-2016-18:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.19.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	211
176.13.15.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	77
109.253.219.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
79.182.27.147	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
176.13.19.4	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	15
46.121.59.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
85.64.240.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
46.121.28.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.85.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
213.8.204.18	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.8.204.18	Block	4
176.13.1.11	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
37.26.146.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.117.26.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.65.154.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.4.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.178.197.140	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	3
37.26.148.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.178.150.48	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
37.239.149.183	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	2
176.13.14.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.3.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.27.106.69	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.27.106.69	Block	2
80.178.197.140	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 80.178.197.140	Block	2
176.228.188.9	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	2
46.19.85.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.178.204.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.228.188.9	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
2.54.26.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
165.225.72.85	United States	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.228.188.9	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.111.38.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
176.228.188.9	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	2
2.54.185.191	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.185.191	Block	2
82.81.10.126	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	2
176.228.188.9	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	2
176.228.188.9	Israel	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	2
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
176.13.19.4	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
87.68.159.124	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
212.179.10.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/1/	Block	1
84.111.38.42	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 84.111.38.42	Block	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	1
66.249.78.28	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
176.13.12.24	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$7 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
80.179.196.168	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/mi	Block	1
176.228.188.9	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding kÖ°×‘Ãž5â€?×°Â?Â¿[[#31]]-Âš•h{ÃŠ Â?a[[#3]]Ö·d[[#27]][[#30]]×´95}Â?×?u5%Â©)]!×?Ö¶[[#3]][[#15]]Â£[[#4]]d[[#5]]Â»oy×²Æ'×ž ÖµÂ¡×£5p[[#17]]×?Ö°Ã»[[#31]]Â³[[#27]]Â©ÂµÃ·Â¿"×§[[#24]]0×ƒw:× hÂ¥Ëœ ×°ÃŠ>Â¨_[[#4]]Ö¸da[[#22]]v×,bÂŸÖ»×–×¤×¤Ö¿nÖ¸Â´ÂŽ Â¦u%o×´Ö¼[[#20]]4"7[[#14]]×œ^ÂŽ[[#0]]se3â,¬Â¨×š 'Â?[[#28]][[#17]]z[[#16]][[#18]][[#2]]×±×,b×€ÃŸÂ¦lÂ?tÂŒÖ¼[[#22]]'#â€™ h[[#5]]× [[#17]])^	Block	1
149.78.30.36	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1

02-04-2016-17:04:01 to 02-04-2016-18:04:01