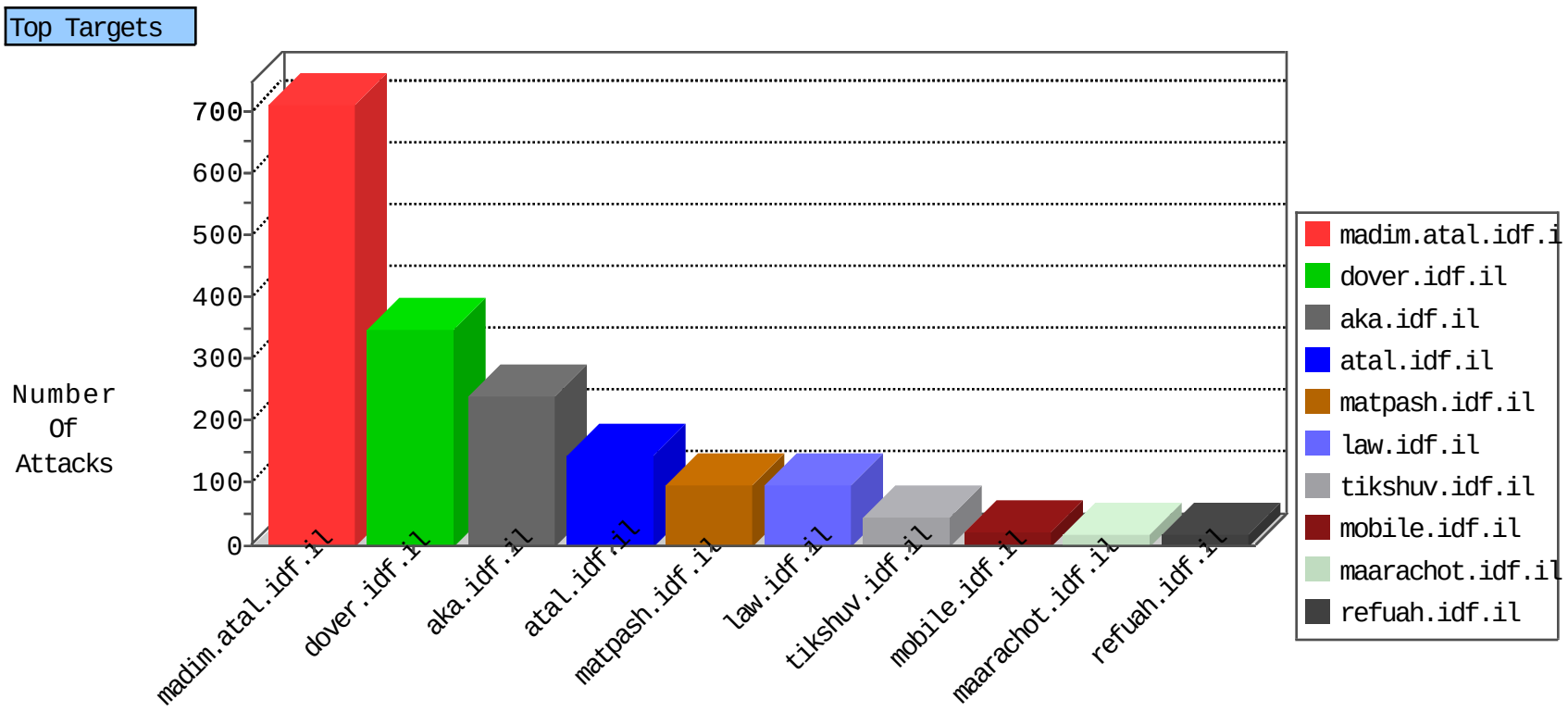
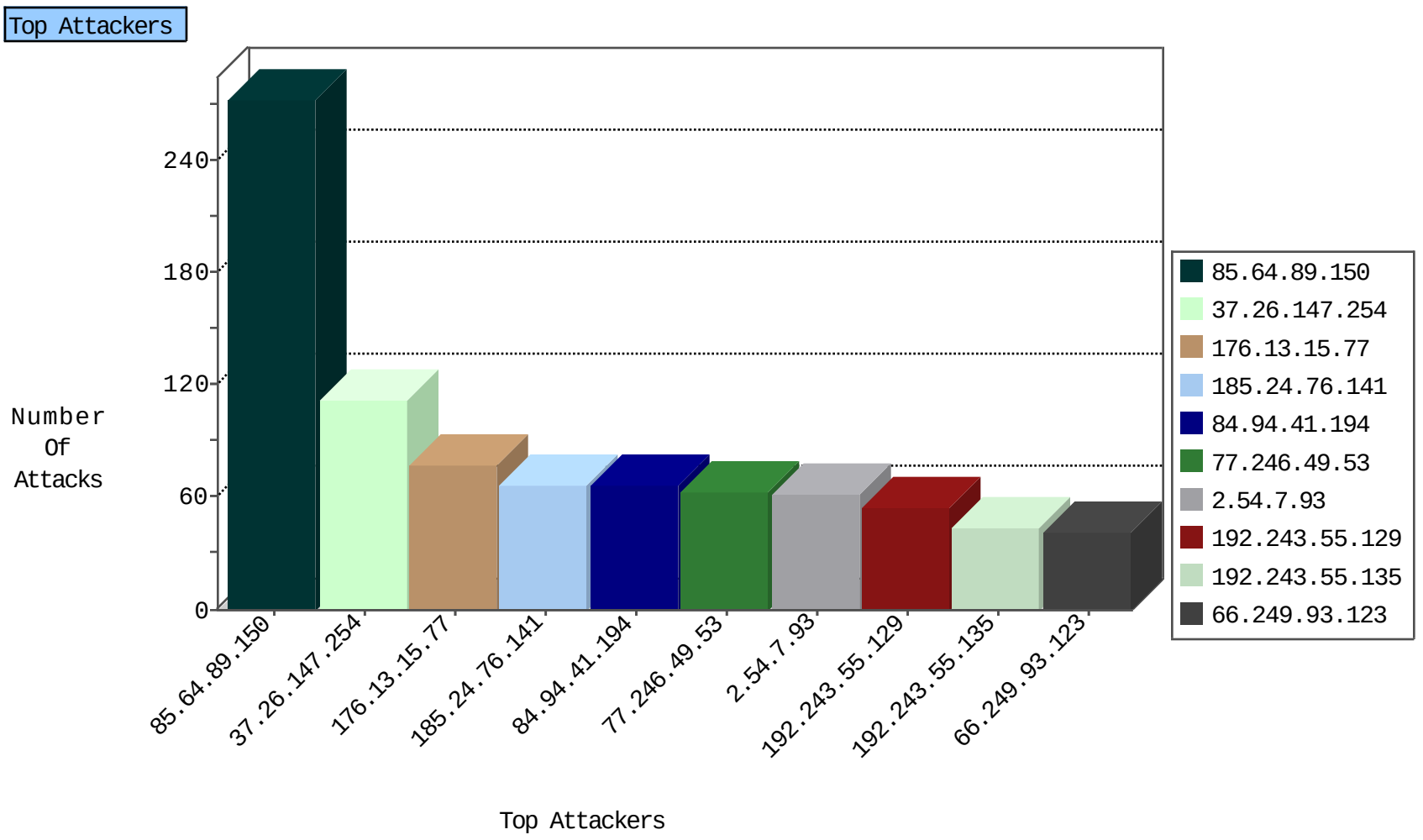
02-18-2016-20:04:06 to 02-18-2016-21:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-18-2016-20:04:06 to 02-18-2016-21:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.133.208	Canada	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	3
198.84.193.7	Canada	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3
190.237.143.243	Peru	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
190.40.69.17	Peru	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
190.40.69.17	Peru	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

02-18-2016-20:04:06 to 02-18-2016-21:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.62.87	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	18
5.29.118.44	Israel	147.237.72.166	aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	4
85.64.249.42	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
109.65.72.158	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
5.29.118.44	Israel	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1

02-18-2016-20:04:06 to 02-18-2016-21:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.133.236	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.93.67	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
180.97.106.162	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.161	147.237.0.19	China	madim.atal.idf.i	ET SCAN Potential SSH Scan	1
104.154.93.51	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
85.93.5.65	147.237.77.74	Germany	law.idf.il	ET SCAN Potential SSH Scan	1
84.111.5.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.192.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.216.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
190.104.75.148	147.237.76.34	Argentina	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.97.106.161	147.237.72.14	China	dover.idf.il(old	ET SCAN Potential SSH Scan	1
107.189.73.204	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 4096	1
88.157.203.66	147.237.77.216	Portugal	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.96.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.121.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
192.243.55.129	147.237.77.216	Dominica	dover.idf.il	portscan: TCP Distributed Portscan	1

02-18-2016-20:04:06 to 02-18-2016-21:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	41
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	27
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	27
77.246.49.53	Zimbabwe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.93.127	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	17
41.102.134.13	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
77.246.49.53	Zimbabwe	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
109.186.184.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
37.26.147.147	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.210.187.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.246.49.53	Zimbabwe	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
77.246.49.53	Zimbabwe	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
5.102.195.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.186.184.176	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
80.246.130.172	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
109.186.184.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
109.186.184.176	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
37.46.39.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.176.54.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.163.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
109.64.176.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.186.184.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.54.0.71	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
77.246.49.53	Zimbabwe	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	5
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.135	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
188.120.154.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
190.237.143.243	Peru	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

02-18-2016-20:04:06 to 02-18-2016-21:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.89.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	127
85.64.89.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
37.26.147.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	78
176.13.15.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
2.54.7.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
185.24.76.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
84.94.41.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
85.64.89.150	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 85.64.89.150	Block	41
46.121.244.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
37.26.147.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	33
84.94.41.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	22
109.66.54.242	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 109.66.54.242	Block	17
185.24.76.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	6
197.38.197.170	Egypt	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	5
176.13.15.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	5
134.249.54.139	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/mazi/	Block	5
197.38.197.170	Egypt	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	5
84.108.66.212	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 84.108.66.212	Block	4
79.182.174.30	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	4
79.182.174.30	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	4
5.29.118.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.29.118.44	Block	4
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
37.142.64.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.177.240.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.102.7.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.119.123.238	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/mazi/	Block	3
62.219.225.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
217.132.111.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.0.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
149.78.54.60	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	1
85.64.89.150	Israel	147.237.0.19	madim.atal.idf.i	Too Many 403: Response Code per Session	Block	1
80.246.130.211	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
66.249.66.36	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
62.122.240.191	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
109.160.142.78	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
5.29.118.44	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
197.38.197.170	Egypt	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/xmlrpc.php	Block	1
184.168.192.107	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
157.55.39.164	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
207.46.13.90	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/kapatz/Ã‚â€“Ã‚â€?	Block	1
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/yassin2.wmv http:/apexvid.com/t8p746bln3qp	Block	1
82.166.239.163	Israel	147.237.76.30	himush.idf.il	Multiple Unauthorized URL Access from 82.166.239.163	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-12321-en	Block	1
178.165.76.75	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
109.253.140.46	Israel	147.237.72.166	aka.idf.il	Too Many Cookies in a Request - 113 cookies	Block	1
62.219.225.130	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.219.225.130	Block	1
84.108.66.212	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf	Block	1
197.38.197.170	Egypt	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1

02-18-2016-20:04:06 to 02-18-2016-21:04:06