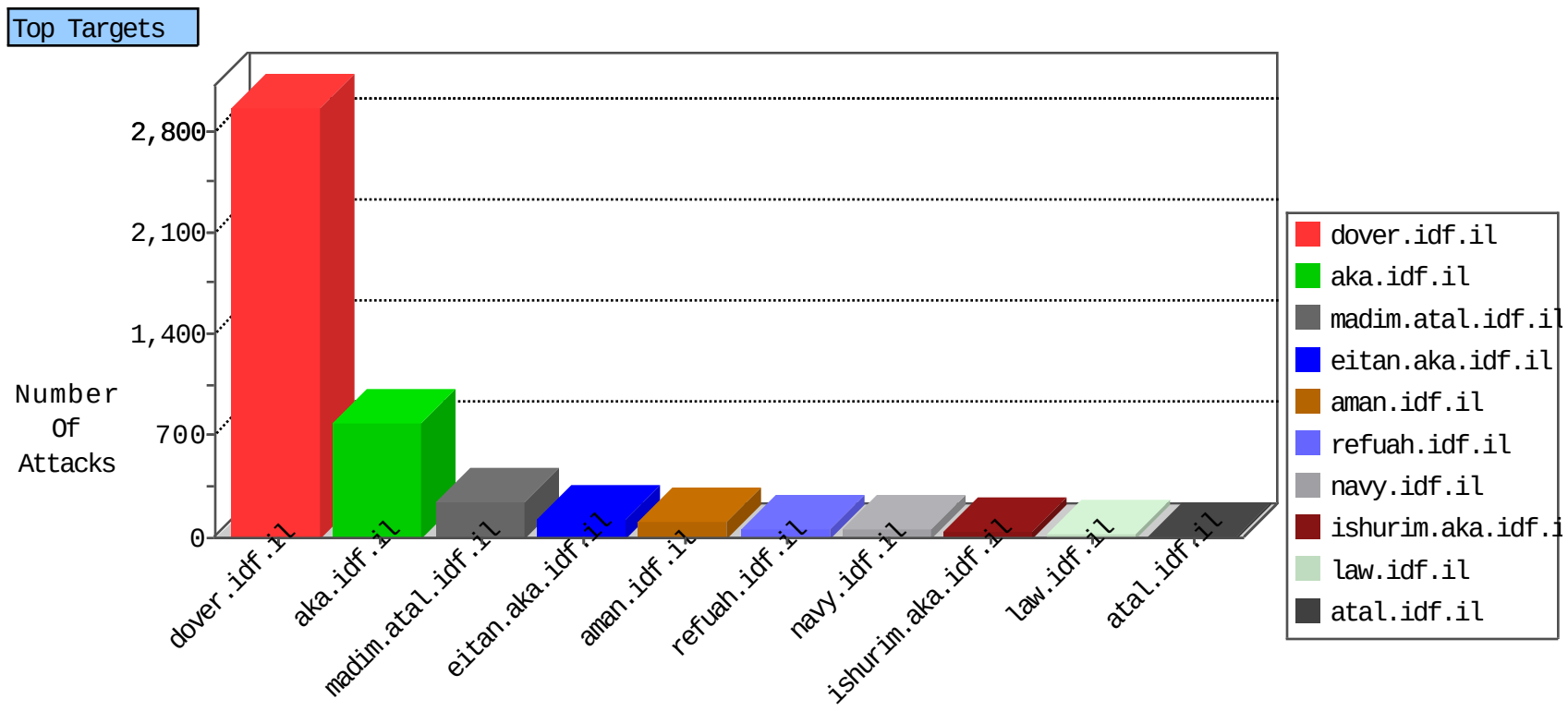
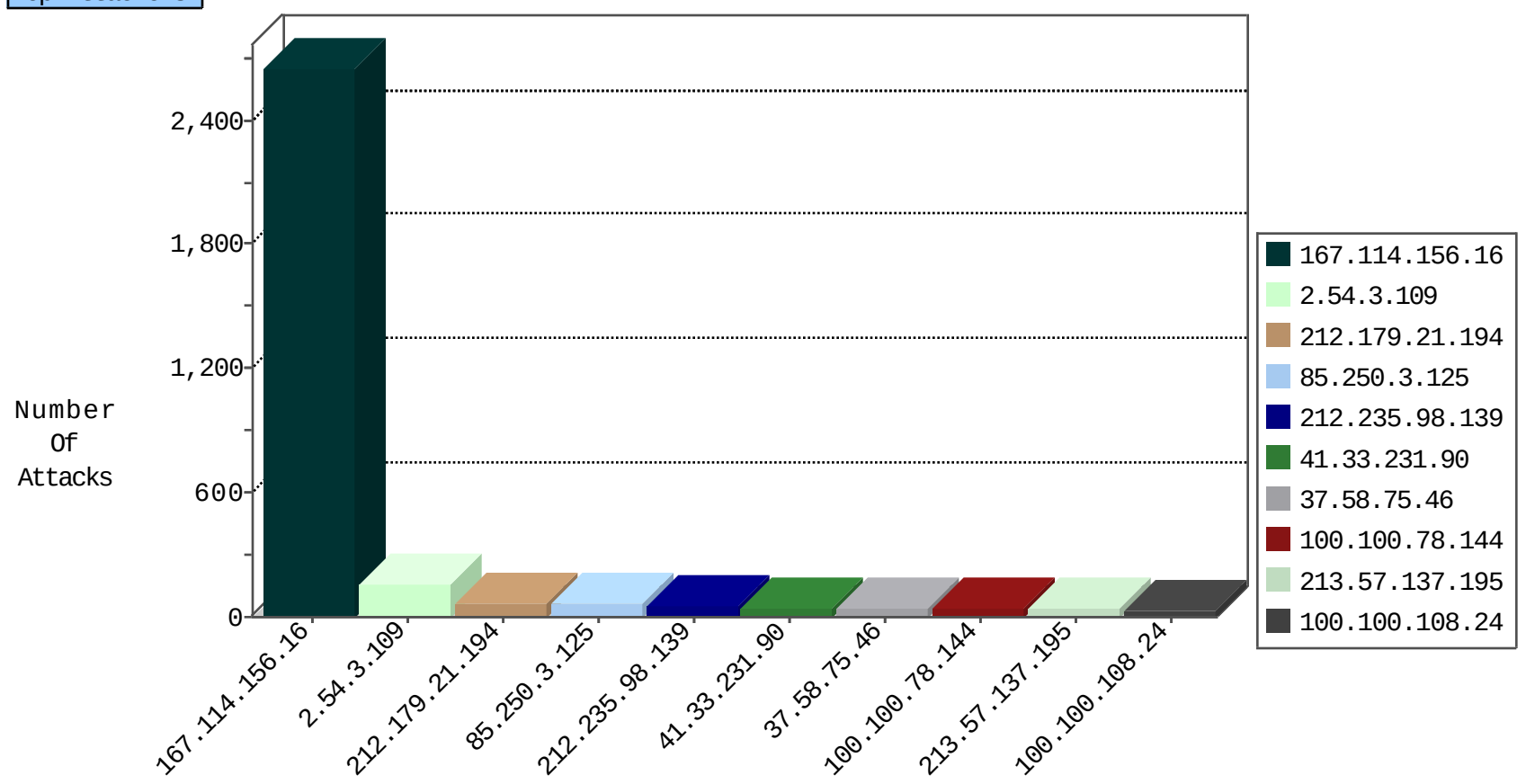
11-30-2015-16:04:04 to 11-30-2015-17:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-30-2015-16:04:04 to 11-30-2015-17:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3392
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
79.176.21.114	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
192.118.132.185	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
192.118.132.185	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
2.54.166.217	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
94.102.49.210	Netherlands	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.210	Netherlands	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
79.182.134.5	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
94.102.49.210	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
198.48.92.104	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

11-30-2015-16:04:04 to 11-30-2015-17:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
85.64.38.129	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
95.86.116.24	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
188.165.15.127	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-30-2015-16:04:04 to 11-30-2015-17:04:04

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	3
185.24.76.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.224.168	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.63.239.135	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
58.63.239.135	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
5.29.153.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.61.109.189	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
58.63.239.135	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
46.121.83.101	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.28.145.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.76.197	United States	e.himush.idf.il	ET DROP Dshield Block Listed Source	1

11-30-2015-16:04:04 to 11-30-2015-17:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	55
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
100.100.6.21		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
100.100.78.144		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
213.57.137.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
213.57.129.222	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
100.100.108.24		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
213.57.137.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
46.19.85.248	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.172	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
100.100.108.24		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
100.100.78.144		147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	12
100.100.9.206		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
159.203.86.106	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
100.100.103.221		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
93.173.4.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
85.250.3.125	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
109.67.139.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.183.114.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.248	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
80.179.40.30	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
213.57.131.24	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
62.219.151.179	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
213.57.131.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
80.179.40.30	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
212.179.21.194	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.180.224.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.167	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.58.75.46	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	6
2.54.171.231	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
100.100.0.64		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.52.167.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.58.75.46	Netherlands	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	6
89.138.76.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
188.120.148.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.88.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
65.49.14.72	Anonymous Proxy	147.237.72.166	aka.idf.il	drop		drop	6
37.58.75.46	Netherlands	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
185.3.144.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.44.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.64.173.190	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
199.203.240.133	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.160.191.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.58.75.46	Netherlands	147.237.77.205	prisha.idf.il	drop	SAM rule	drop	6
213.8.44.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.158	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.3.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	53
85.250.3.125	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	50
2.54.3.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	42
176.12.144.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
2.54.6.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
185.24.76.151	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	12
176.13.7.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
46.19.85.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
46.19.85.6	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	6
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	6
213.57.241.169	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	5
87.69.247.172	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mani/sachar	Block	4
79.183.119.245	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
176.13.1.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.12.141.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.183.21.24	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
31.44.134.156	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
185.32.179.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
50.87.203.247	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
37.26.147.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.47.254.18	Germany	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
79.177.192.52	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
104.197.3.164	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
95.85.19.27	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
212.199.224.24	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 212.199.224.24	Block	3
104.155.4.193	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
198.143.135.82	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
213.57.241.169	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
192.163.209.98	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
198.46.81.3	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
31.47.254.18	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
50.87.203.247	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
104.197.3.164	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
95.85.19.27	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
207.46.13.91	United States	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
149.78.155.132	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
104.155.4.193	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
198.143.135.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
31.47.254.18	Germany	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
2.54.3.109	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
207.46.13.91	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
198.46.81.3	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
85.250.3.125	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 85.250.3.125	Block	2
8.37.70.123	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/&usg=alkjrhgbuwxutshzsppdgyprwhwme8dp0w	Block	2
104.197.3.164	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2

11-30-2015-16:04:04 to 11-30-2015-17:04:04