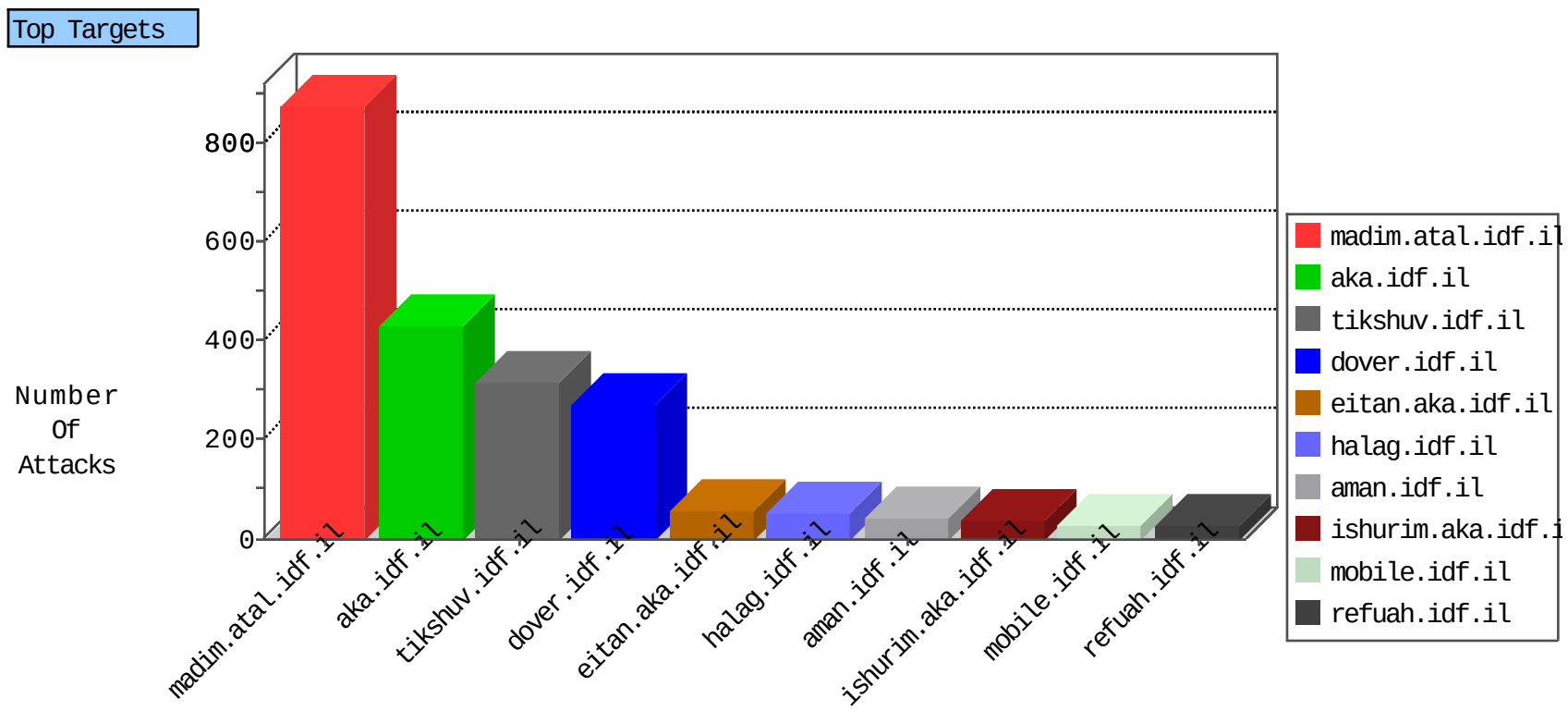
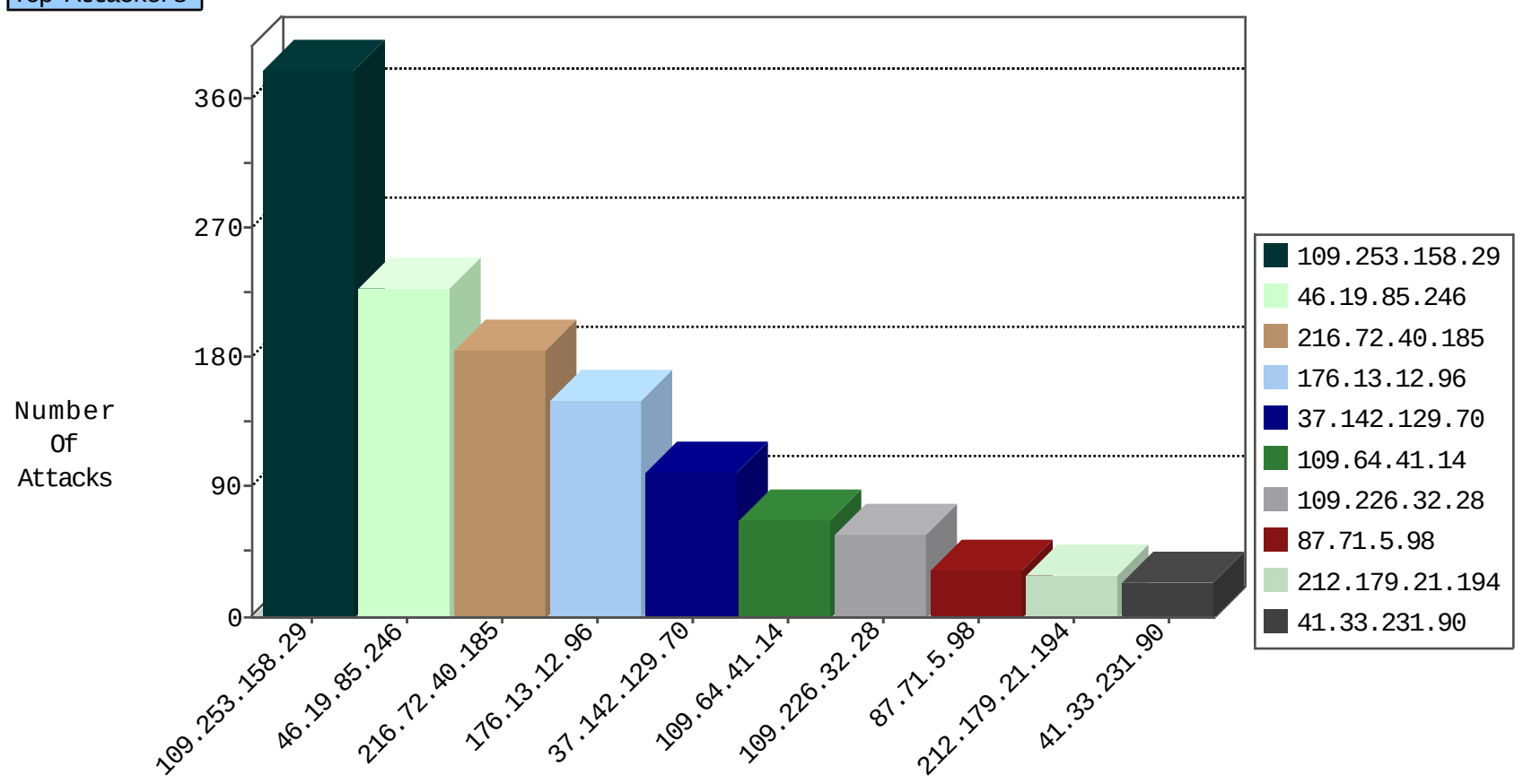
02-16-2016-15:04:09 to 02-16-2016-16:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-16-2016-15:04:09 to 02-16-2016-16:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	140
77.171.50.176	Netherlands	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
212.179.64.162	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
217.31.55.69	Czech Republic	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.176.127.112	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
173.208.206.203	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
185.130.5.224		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
79.178.200.40	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1

02-16-2016-15:04:09 to 02-16-2016-16:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
49.246.230.40	China	147.237.77.216	dover.idf.il	8479: HTTP: Suspicious HTTP Request	Block	2
92.29.219.30	United Kingdom	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	2
51.255.155.83	United Kingdom	147.237.77.216	dover.idf.il	C196: HTTP: Block admin login to gov.il sites ?q=user	Block	1
69.30.210.242	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1

02-16-2016-15:04:09 to 02-16-2016-16:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.26.148.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.77.226	United States	www.chamatz.aka.idf.il	ET DROP Dshield Block Listed Source	1
185.130.5.179	147.237.77.234		halag.idf.il	ET SCAN Potential SSH Scan	1
93.113.125.11	147.237.76.177	Romania	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.61.152	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.200.40	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
64.47.186.53	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.117.132.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.47.32.112	147.237.77.216	Brazil	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
109.64.151.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.130.188.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.67.193	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.131.123	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.126.229.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.137.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.25.84.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-16-2016-15:04:09 to 02-16-2016-16:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.226.32.28	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
212.179.21.194	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
40.141.115.140	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
80.246.133.7	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
46.19.85.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
199.203.211.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
41.234.223.182	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.213	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
70.214.68.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
41.254.8.151	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
70.214.68.133	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.143.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.213	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.3.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.110.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.135.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
70.214.68.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
149.78.24.54	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.167	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.26.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
41.254.8.151	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.52.191.231	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.26.242	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.54.26.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.126	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.26.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.8.122.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	4
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
192.115.248.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.173	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
41.234.223.182	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.203.93.50	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
41.234.223.182	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
46.19.85.173	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.154.41.13	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.210.187.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.28.189.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.144.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.197	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.177.148.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.51.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.7.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.191	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

02-16-2016-15:04:09 to 02-16-2016-16:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
216.72.40.185	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	186
109.253.158.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	184
109.253.158.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	122
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.246	Block	118
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
176.13.12.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	103
37.142.129.70	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning	Block	101
109.253.158.29	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 109.253.158.29	Block	75
109.64.41.14	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	67
176.13.12.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	47
87.71.5.98	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	33
85.64.176.95	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	23
109.253.206.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
37.26.148.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
80.246.138.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
192.117.138.211	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	10
80.246.137.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
46.19.85.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
79.177.58.171	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.177.58.171	Block	5
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
2.54.63.250	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.63.250	Block	5
51.255.155.83	United Kingdom	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	4
66.249.83.155	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.19.85.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
51.255.155.83	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 51.255.155.83	Block	4
93.186.16.246	South Africa	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
80.246.136.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.16.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	3
79.176.127.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.176.127.112	Block	3
80.246.137.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.147.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
149.88.108.130	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.88.108.130	Block	3
109.253.223.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.31.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.136.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.176.127.112	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
92.198.27.76	Germany	147.237.77.74	law.idf.il	Distributed Parameter Type Violation on www.law.idf.il/327-en/patzar.aspx parameter PageNum	Block	2
2.54.145.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.52.185.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
93.186.16.243	South Africa	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
51.255.155.83	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
66.249.83.158	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.19.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
149.88.108.130	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
79.178.200.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2

02-16-2016-15:04:09 to 02-16-2016-16:04:09