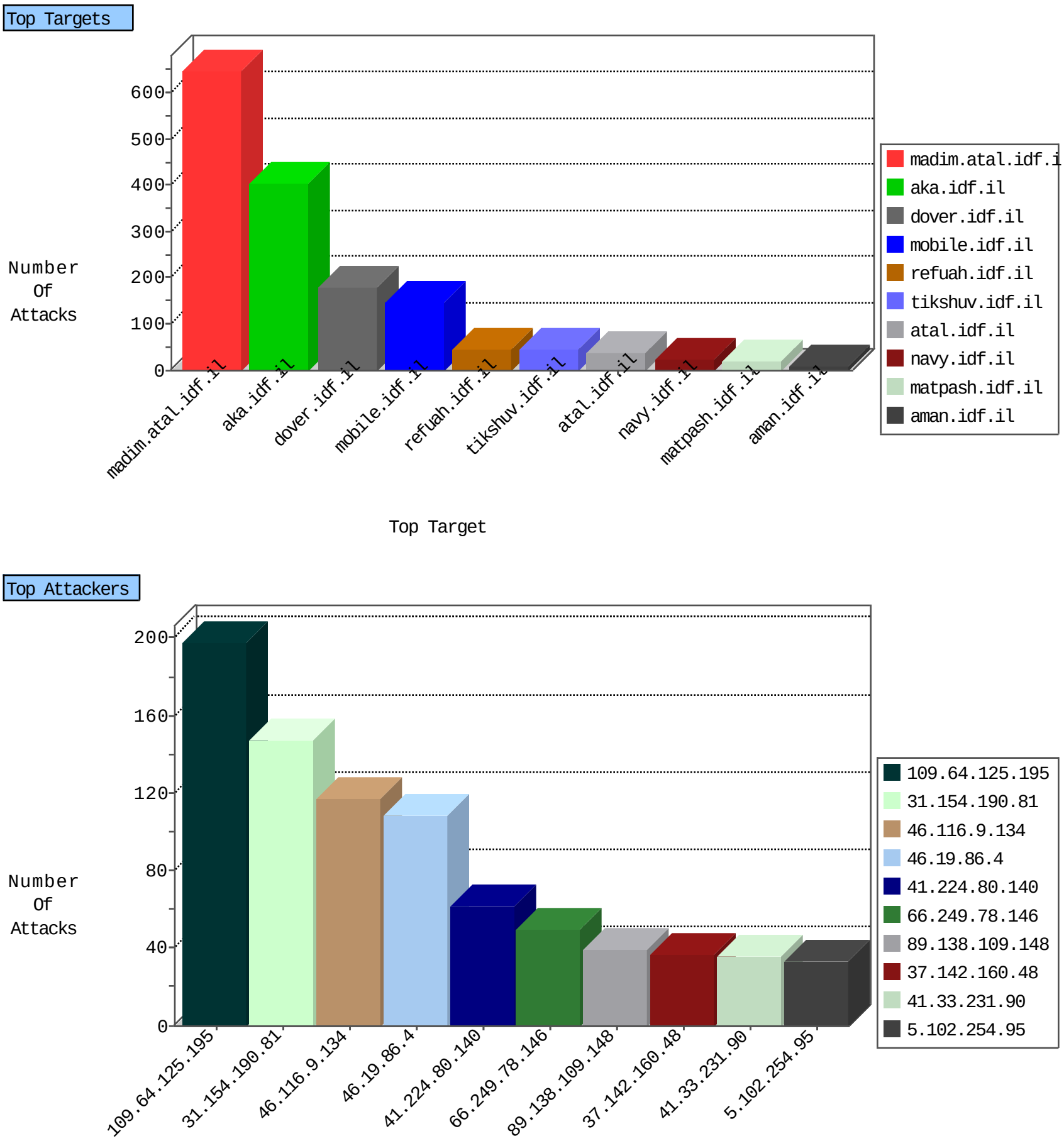
02-27-2016-21:04:09 to 02-27-2016-22:04:09

IDF Under Attack Daily Report



02-27-2016-21:04:09 to 02-27-2016-22:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
82.145.223.105	Europe	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	2
185.130.5.196		147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
64.89.188.181	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
205.209.185.11	United States	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
94.237.25.247	Finland	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
185.130.5.196		147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
68.63.80.220	United States	147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	1
105.154.69.57	Morocco	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.196		147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.196		147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
64.89.188.177	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.130.5.196		147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
83.136.253.223	United Kingdom	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1

02-27-2016-21:04:09 to 02-27-2016-22:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.182.247	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.65.108.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
61.135.189.121	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
89.138.109.148	Israel	147.237.72.166	aka.idf.il	C1000014: HTTP: Malicous UserAgent FOCA	Block	2
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

02-27-2016-21:04:09 to 02-27-2016-22:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.81.175	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.79.75	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
213.57.44.158	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.11.201.3	147.237.76.38	Italy	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
151.11.201.3	147.237.76.38	Italy	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
50.87.144.145	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
213.238.176.44	147.237.72.217	Turkey	e.idf.il	ET SCAN NMAP -sS window 1024	1
151.11.201.3	147.237.76.38	Italy	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
115.28.218.77	147.237.72.167	China	ishurim.aka.idf.i	ET SCAN NMAP -sS window 1024	1
49.205.32.125	147.237.0.34	India	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-27-2016-21:04:09 to 02-27-2016-22:04:09

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
89.138.109.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
87.69.194.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
149.88.253.13	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
37.142.244.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
109.253.142.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.81.175	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	14
37.142.195.192	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
37.142.160.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
37.142.160.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
37.142.160.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
82.166.240.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.238	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	10
41.224.80.140	Tunisia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.183.16.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.177.244.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
41.224.80.140	Tunisia	147.237.0.34	tikshuv.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.108.234.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.168.119	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.142.195.192	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
37.26.146.129	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.117.12.217	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
37.142.134.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.65.38.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.86.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.69.133.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
109.66.194.7	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
188.161.113.106	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
84.94.66.175	Israel	147.237.0.34	tikshuv.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
109.64.16.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
66.249.81.179	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
213.8.204.53	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.195.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.142.200.216	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.142.200.216	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
84.94.66.175	Israel	147.237.0.34	tikshuv.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
37.142.136.98	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
85.64.243.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.168.216.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.133.8	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
77.125.255.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.238	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3

02-27-2016-21:04:09 to 02-27-2016-22:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.125.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	198
31.154.190.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	148
46.116.9.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	117
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	109
5.102.254.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
66.249.78.146	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	26
2.54.191.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	17
41.224.80.140	Tunisia	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 41.224.80.140	Block	13
41.224.80.140	Tunisia	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 41.224.80.140	Block	13
41.224.80.140	Tunisia	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 41.224.80.140	Block	8
89.138.109.148	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.138.109.148	Block	8
149.88.253.13	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
5.102.242.23	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 5.102.242.23	Block	6
87.69.194.195	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
109.67.146.3	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	6
41.224.80.140	Tunisia	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 41.224.80.140	Block	5
2.54.177.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
5.102.242.23	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	4
109.253.142.134	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
82.166.240.201	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
84.108.128.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.10.68	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.140.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.65.75.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	3
41.43.22.89	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.79.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	3
5.28.165.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.177.229.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.29.230.226	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
37.26.147.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.148.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
41.224.80.140	Tunisia	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 41.224.80.140	Block	2
5.29.197.230	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
79.179.27.232	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.179.27.232	Block	2
41.239.12.83	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.150.249.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.29.230.226	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 5.29.230.226	Block	2
109.253.216.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.67.176.124	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
89.138.109.148	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.....f0c4	Block	1
2.54.6.210	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
79.179.137.95	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
207.46.13.102	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/dynamic_map/dynamic_map.aspx	Block	1
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.81.130	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
5.29.84.137	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl17 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in www.aka.idf.il/lomdim/forum/asp/showforum.asp	None	1
46.19.85.150	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 46.19.85.150	Block	1

02-27-2016-21:04:09 to 02-27-2016-22:04:09