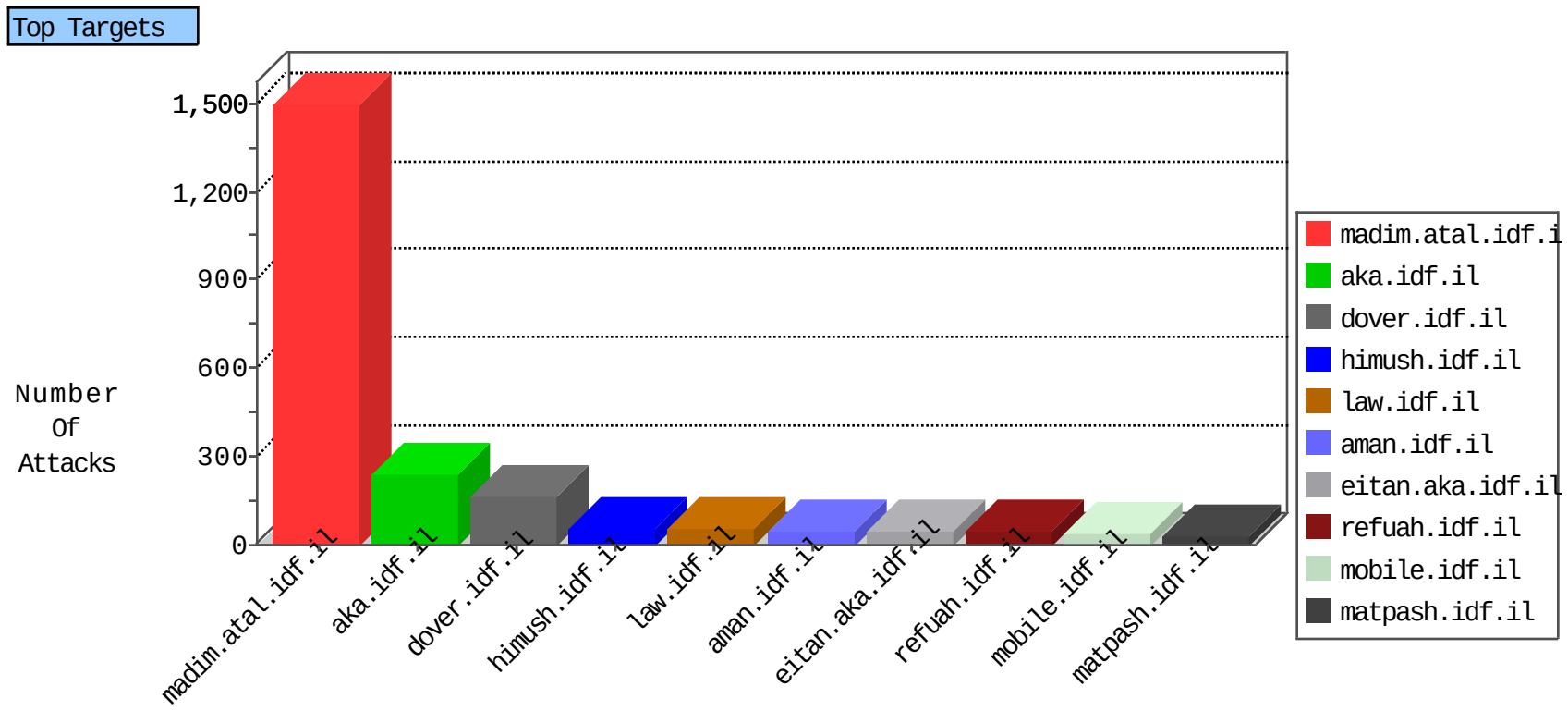
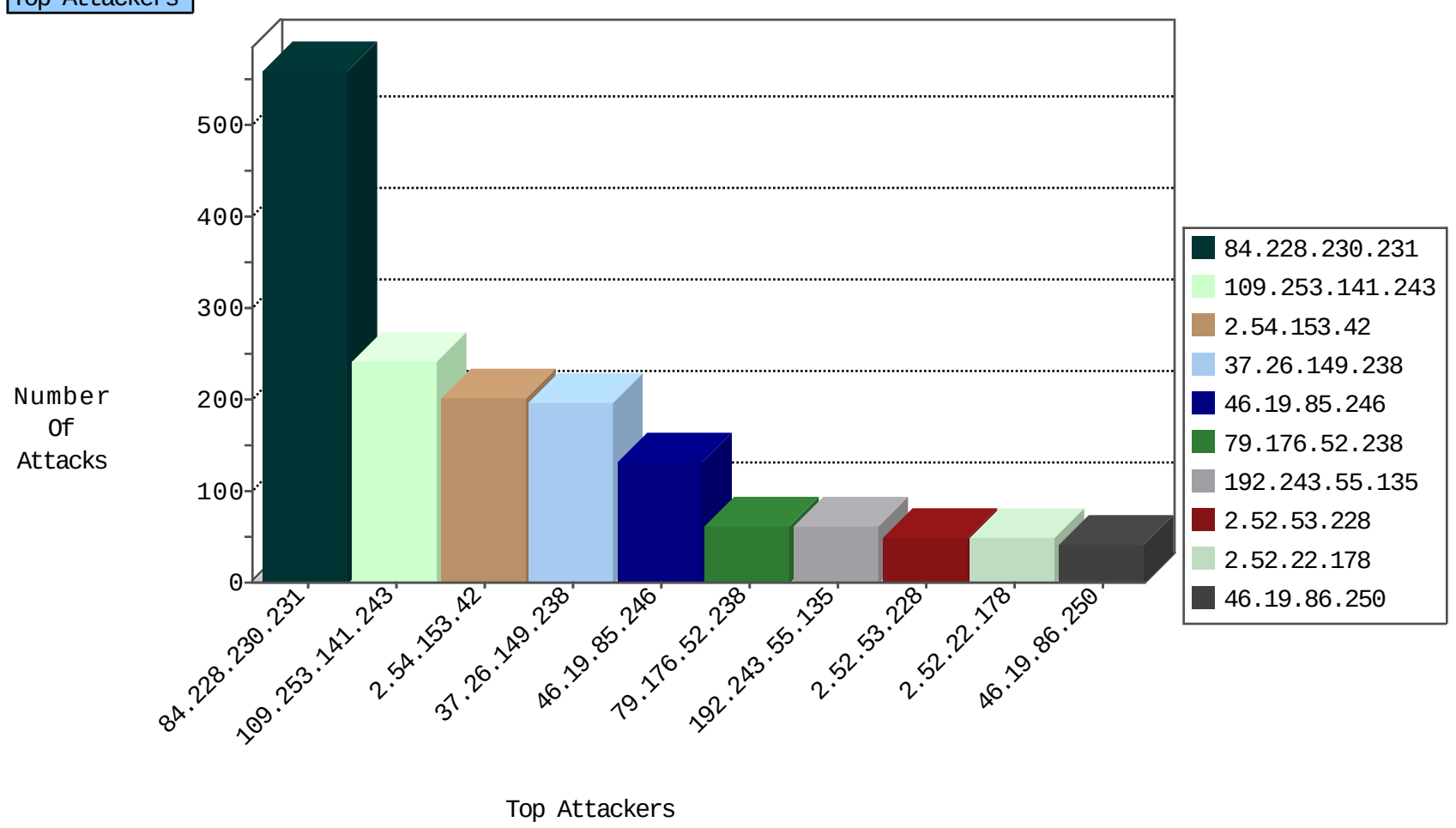
02-20-2016-21:04:00 to 02-20-2016-22:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-20-2016-21:04:00 to 02-20-2016-22:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.93.126.203	Ukraine	147.237.76.31	nakchal.idf.il	L4 Source or Dest Port Zero	drop	2
95.27.15.125	Russian Federation	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	1
80.93.126.203	Ukraine	147.237.8.24	e.lifestyle.idf.il	L4 Source or Dest Port Zero	drop	1
80.93.126.203	Ukraine	147.237.76.39	mobile.meitav.idf.il	L4 Source or Dest Port Zero	drop	1
80.93.126.203	Ukraine	147.237.72.14	dover.idf.il(old)	L4 Source or Dest Port Zero	drop	1
80.93.126.203	Ukraine	147.237.76.147	chinuch.aka.idf.il	L4 Source or Dest Port Zero	drop	1
80.93.126.203	Ukraine	147.237.76.197	e.himush.idf.il	L4 Source or Dest Port Zero	drop	1
80.93.126.203	Ukraine	147.237.76.38	e.e.meitav.idf.il	L4 Source or Dest Port Zero	drop	1

02-20-2016-21:04:00 to 02-20-2016-22:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.88.178.95	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
108.168.219.174	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
87.69.37.73	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
174.34.135.242	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	2
62.210.148.246	France	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	2
79.181.37.46	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
157.55.39.216	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
51.255.155.83	United Kingdom	147.237.77.216	dover.idf.il	C1000196: HTTP: Block admin login to gov.il sites ?q=user	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.97	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1

02-20-2016-21:04:00 to 02-20-2016-22:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
108.168.219.174	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
37.26.149.238	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
91.201.236.114	147.237.76.86	Ukraine	navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.177.131.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.126.58.83	147.237.0.16	Taiwan	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
51.255.155.83	147.237.77.216	United Kingdom	dover.idf.il	SERVER-WEBAPP admin.php access	1
220.231.195.122	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.76.86	Ukraine	navy.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.237.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
74.201.85.87	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
58.186.113.166	147.237.76.148	Vietnam	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
37.46.43.32	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
5.199.164.208	147.237.77.216	Lithuania	dover.idf.il	Tehila - Perl LWP with fake user agent	1
220.231.195.122	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
220.231.195.122	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1

02-20-2016-21:04:00 to 02-20-2016-22:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.52.22.178	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
213.8.204.27	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
79.181.244.30	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
109.253.131.41	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
109.253.159.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.228.230.231	Bulgaria	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
79.182.39.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.182.39.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.176.224.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.135	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
95.27.15.125	Russian Federation	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
82.102.234.69	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.102.195.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.163	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
79.181.48.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.109.3	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.187.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.8.76.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.175.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.145.168	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.86.83	Israel	147.237.72.166	aka.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	Invalid ACK number	monitor	6
5.102.195.159	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.140	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.253.159.77	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.64.172.169	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
188.161.19.83	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
46.117.192.21	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
85.64.172.169	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.135	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
213.57.224.33	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	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
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.22.135.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.159.77	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
31.210.187.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.168.197.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.34.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.210.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.126.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.7.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.23	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

02-20-2016-21:04:00 to 02-20-2016-22:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.228.230.231	Bulgaria	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	287
84.228.230.231	Bulgaria	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	154
109.253.141.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	121
37.26.149.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
2.54.153.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
109.253.141.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
84.228.230.231	Bulgaria	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
2.54.153.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	95
37.26.149.238	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.149.238	Block	82
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
79.176.52.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	52
2.52.53.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	49
46.19.86.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
109.253.141.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	15
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	11
37.26.149.238	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 37.26.149.238	Block	6
213.57.49.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
79.182.39.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.179.197.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.182.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.65.149.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.28.182.213	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.52.144.68	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.109.156.104	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	2
5.199.164.208	Lithuania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
79.178.4.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.26.182.31	Europe	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https:/twitter.com/	Block	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2113-he/cogat.aspx	Block	1
46.121.75.107	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
79.178.64.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
51.255.155.83	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/administrator/	Block	1
188.146.72.58	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
109.66.22.29	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
80.246.130.32	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
5.102.202.158	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
78.154.170.2	Ukraine	147.237.72.166	aka.idf.il	Unknown Parameter amp;pagenum in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
128.232.110.28	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
51.255.155.83	United Kingdom	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
84.228.230.231	Bulgaria	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.178.132.119	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$71 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
65.55.210.192	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	1
109.253.131.41	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
157.55.39.159	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
51.255.155.83	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
87.68.145.168	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
5.199.164.208	Lithuania	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.199.164.208	Block	1

02-20-2016-21:04:00 to 02-20-2016-22:04:00