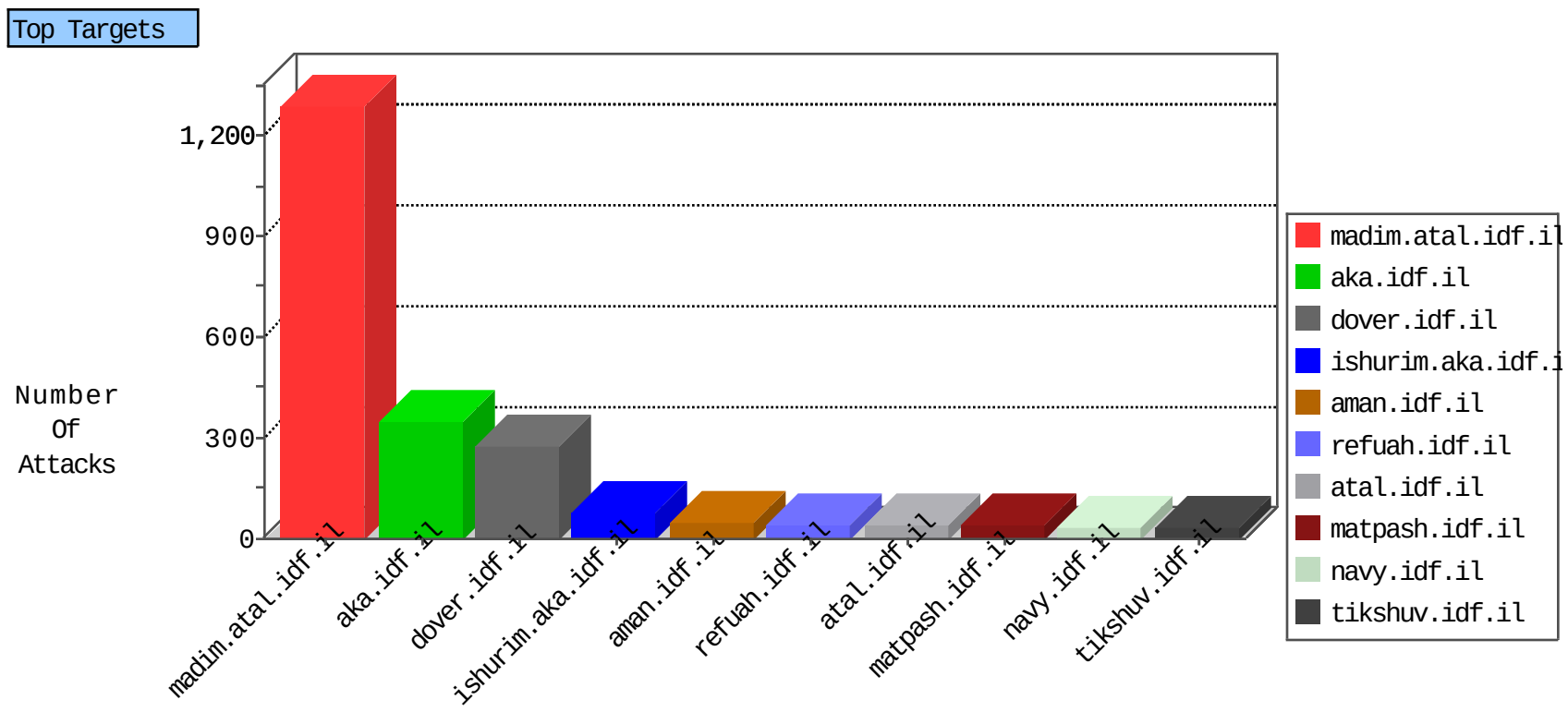
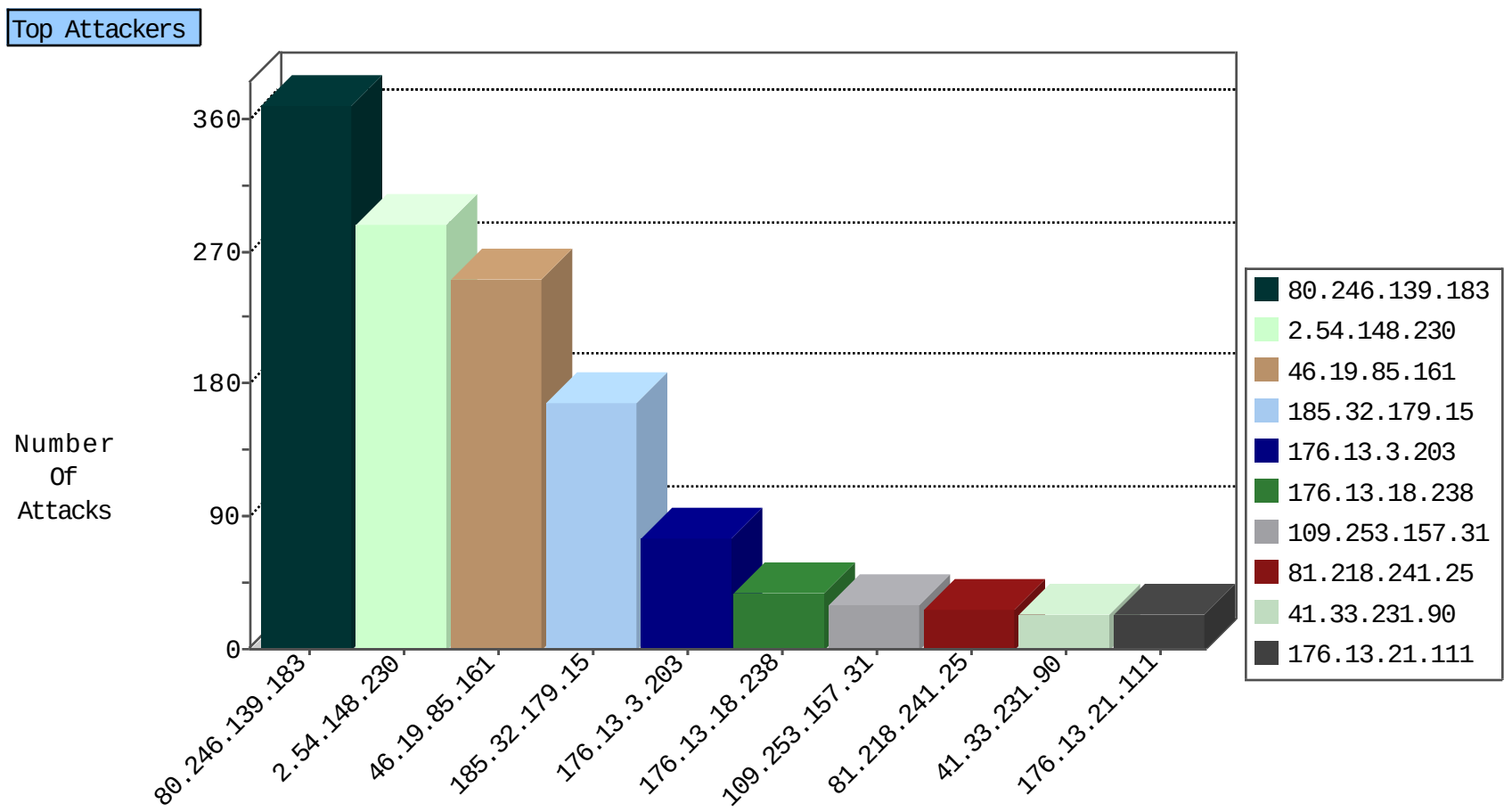
02-22-2016-11:04:04 to 02-22-2016-12:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-22-2016-11:04:04 to 02-22-2016-12:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	48
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
125.74.116.108	China	147.237.76.147	chinuch.aka.idf.il	Invalid TCP Flags	drop	2
159.104.163.19	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.104.163.20	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.104.163.17	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.104.163.21	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.249.66.33	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
159.104.163.18	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.130.5.201		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
77.87.228.68	Germany	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

02-22-2016-11:04:04 to 02-22-2016-12:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.237.163	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
193.106.206.10	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
79.177.194.221	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
144.76.29.162	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.29.162	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
37.26.149.218	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
89.216.115.6		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	1
5.9.111.70	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1
106.39.60.188	China	147.237.76.176	test.ncore.idf.	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
106.39.60.188	China	147.237.76.177	ncore.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1

02-22-2016-11:04:04 to 02-22-2016-12:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.20.53	147.237.72.156	Israel	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	10
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
79.176.111.210	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.231	147.237.77.176		matpash.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.123.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.193	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.144	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
82.81.47.15	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.66.122	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.105.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.209.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.29.202.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.231	147.237.76.31		nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.20.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.8.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.144	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
84.95.202.76	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.81.11.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.79.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-22-2016-11:04:04 to 02-22-2016-12:04:04

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	24
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	21
176.228.218.6	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	14
194.90.153.133	Israel	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	10
109.65.170.40	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
2.52.156.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.131.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.70	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.131.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.202.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
202.62.98.33	Lao People's Democratic Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.71.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
2.54.55.189	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.7.171	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
199.203.215.1	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.7.171	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.55.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
37.8.53.236	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
2.52.7.171	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
66.249.81.202	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
2.54.55.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
194.90.66.15	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.25.84.200	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	4
149.88.74.165	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.7.171	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.179.238.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.55.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.168.144.255	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.114.23.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.38.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.55.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.166.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.105.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.94.207.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.16.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.191.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.15.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.255.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.225.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.6.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.98	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
185.27.105.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-22-2016-11:04:04 to 02-22-2016-12:04:04

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
2.54.53.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-22-2016-11:04:04 to 02-22-2016-12:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.139.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	210
2.54.148.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	179
80.246.139.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	160
46.19.85.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	156
185.32.179.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	126
2.54.148.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
46.19.85.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
176.13.3.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
185.32.179.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
176.13.18.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
109.253.157.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	26
176.13.21.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
176.13.3.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
46.19.86.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
90.179.91.227	Czech Republic	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 90.179.91.227	Block	14
89.138.68.53	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	10
208.115.111.72	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.111.72	Block	10
195.154.146.225	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	8
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	5
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
2.54.148.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Illegal Response Code	None	4
176.13.18.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
45.79.168.168		147.237.77.176	matpash.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
46.19.85.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	3
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	3
176.13.19.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	3
46.19.86.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.69.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	3
46.19.86.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.160.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	3
2.54.15.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.179.61.123	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https:/twitter.com/	Block	2
77.127.242.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
5.22.131.17	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
207.46.13.193	United States	147.237.72.166	aka.idf.il	Unauthorized Method GET for aka.idf.il/kamlar/contact/default.asp	Block	2
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method b21f02d43b80.1456134211.1.1456134211.1456134211.; in URL _pk_ses.20.8afc=*	Block	2
81.209.177.95	Europe	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/links/links.aspx	Block	2
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	2
37.26.148.242	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403	Block	2
109.253.215.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
2.54.59.0	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.161	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	2
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	2
46.19.86.232	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
188.120.159.212	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	2

02-22-2016-11:04:04 to 02-22-2016-12:04:04