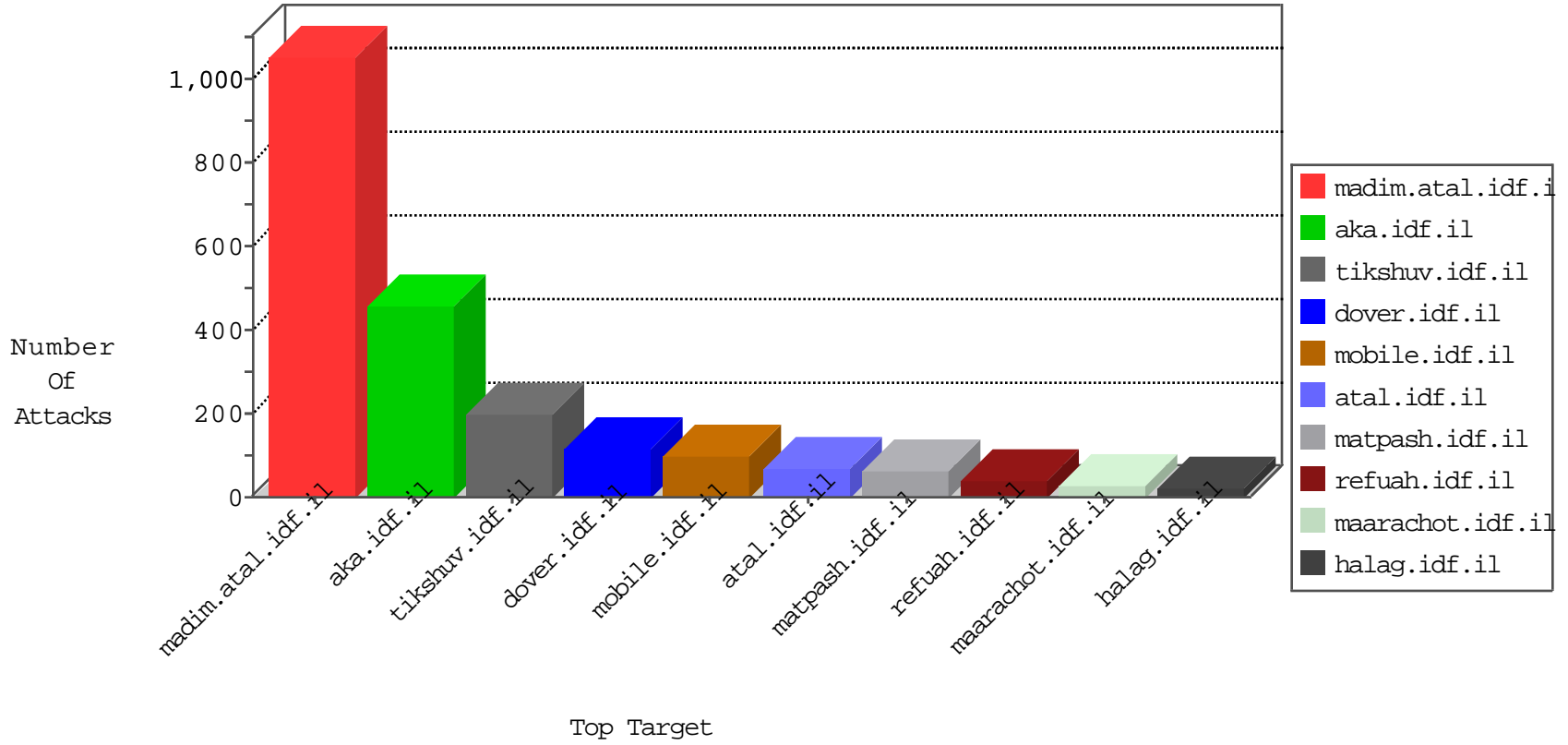


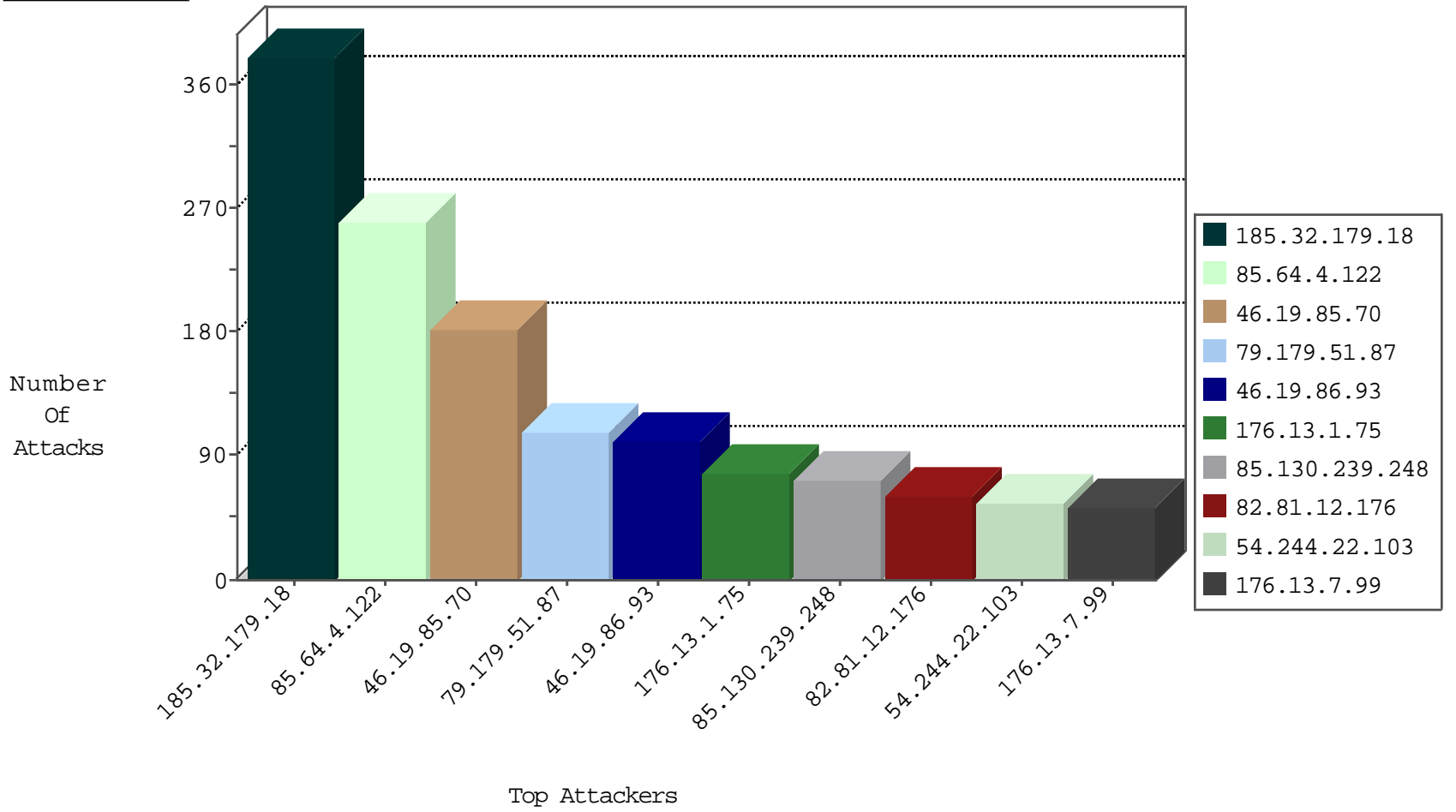
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	60
185.130.5.181		147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.201		147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

01-30-2016-16:04:00 to 01-30-2016-17:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
185.32.179.18	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.78.62	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
1.64.62.70	147.237.72.166	Hong Kong	aka.idf.il	ET SCAN Potential SSH Scan	2
1.64.62.70	147.237.77.178	Hong Kong	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
1.64.62.70	147.237.72.217	Hong Kong	e.idf.il	ET SCAN Potential SSH Scan	2
1.64.62.70	147.237.72.156	Hong Kong	aman.idf.il	ET SCAN Potential SSH Scan	2
75.170.251.3	147.237.77.176	United States	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
1.64.62.70	147.237.77.234	Hong Kong	halag.idf.il	ET SCAN Potential SSH Scan	1
171.251.41.213	147.237.76.30	Vietnam	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
1.64.62.70	147.237.0.34	Hong Kong	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
1.64.62.70	147.237.77.227	Hong Kong	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
158.130.6.191	147.237.77.176	United States	matpash.idf.il	ET SCAN Rapid POP3S Connections - Possible Brute Force Attack	1
146.0.75.114	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
1.64.62.70	147.237.76.202	Hong Kong	e.halag.idf.il	ET SCAN Potential SSH Scan	1
140.112.16.20	147.237.0.34	Taiwan	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
1.64.62.70	147.237.76.197	Hong Kong	e.himush.idf.il	ET SCAN Potential SSH Scan	1
113.171.23.126	147.237.77.178	Vietnam	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
1.64.62.70	147.237.76.148	Hong Kong	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	147.237.76.197	Turkey	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
1.64.62.70	147.237.76.34	Hong Kong	yohalan.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
198.20.69.74	147.237.77.19	United States	law-forum.idf.il	ET DROP Dshield Block Listed Source	1
1.64.62.70	147.237.77.233	Hong Kong	atal.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
1.64.62.70	147.237.0.19	Hong Kong	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
1.64.62.70	147.237.77.212	Hong Kong	e.dover.idf.il	ET SCAN Potential SSH Scan	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
1.64.62.70	147.237.77.19	Hong Kong	law-forum.idf.il	ET SCAN Potential SSH Scan	1
140.112.16.20	147.237.0.34	Taiwan	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
1.64.62.70	147.237.76.201	Hong Kong	e.atal.idf.il	ET SCAN Potential SSH Scan	1
125.27.206.107	147.237.76.30	Thailand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
1.64.62.70	147.237.76.196	Hong Kong	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
113.171.23.126	147.237.72.167	Vietnam	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
1.64.62.70	147.237.76.38	Hong Kong	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
1.64.62.70	147.237.76.31	Hong Kong	nakchal.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	100
85.130.239.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
84.109.228.246	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
109.253.156.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
46.116.84.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.116.79.47	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
213.6.119.94	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	17
79.182.177.33	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
84.109.228.246	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
91.227.71.250	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.189.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.160.147.41	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
109.160.147.41	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
66.102.9.107	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	9
2.52.183.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.6.119.94	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
213.57.178.166	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.192	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.110.211.150	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.193	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.141.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.54.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.117.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
79.180.2.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.125.43		147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.120.223	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.147.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.117.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
84.228.120.223	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.236.158	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.255.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.135.102.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.6.119.94	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	SYN Attack		reject	5
213.6.119.94	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.179.57.94	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	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
5.22.130.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.68.36.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.138.179	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
31.210.186.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
149.78.49.79	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.6.119.94	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

01-30-2016-16:04:00 to 01-30-2016-17:04:00

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.44	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
94.230.86.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	226
85.64.4.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	154
185.32.179.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
79.179.51.87	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	108
85.64.4.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
176.13.1.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	77
176.13.7.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
185.32.179.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	38
2.54.29.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
2.54.180.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
2.52.183.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
46.116.84.34	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
2.54.40.168	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	4
79.176.147.234	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.176.147.234	Block	4
46.120.142.235	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.120.142.235	None	3
46.120.233.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.208.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.40.166	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	3
188.143.232.43	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
85.65.168.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.149.105.229	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	2
2.52.183.157	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.111.103.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
41.82.69.105	Senegal	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
5.29.117.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
109.253.141.42	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
52.7.92.113	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1395-en/dover.aspx	Block	1
85.250.119.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.72.6.178	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
5.255.253.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
177.152.183.70	Brazil	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
80.246.136.169	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/faq.aspx	None	1
77.125.133.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.159.199	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	1
2.54.9.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.228.120.223	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
41.82.69.105	Senegal	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
79.182.147.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.128.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
168.235.206.107	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
2.54.41.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.206.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
52.7.92.113	United States	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1395-en/dover.aspx	Block	1
46.72.6.178	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1