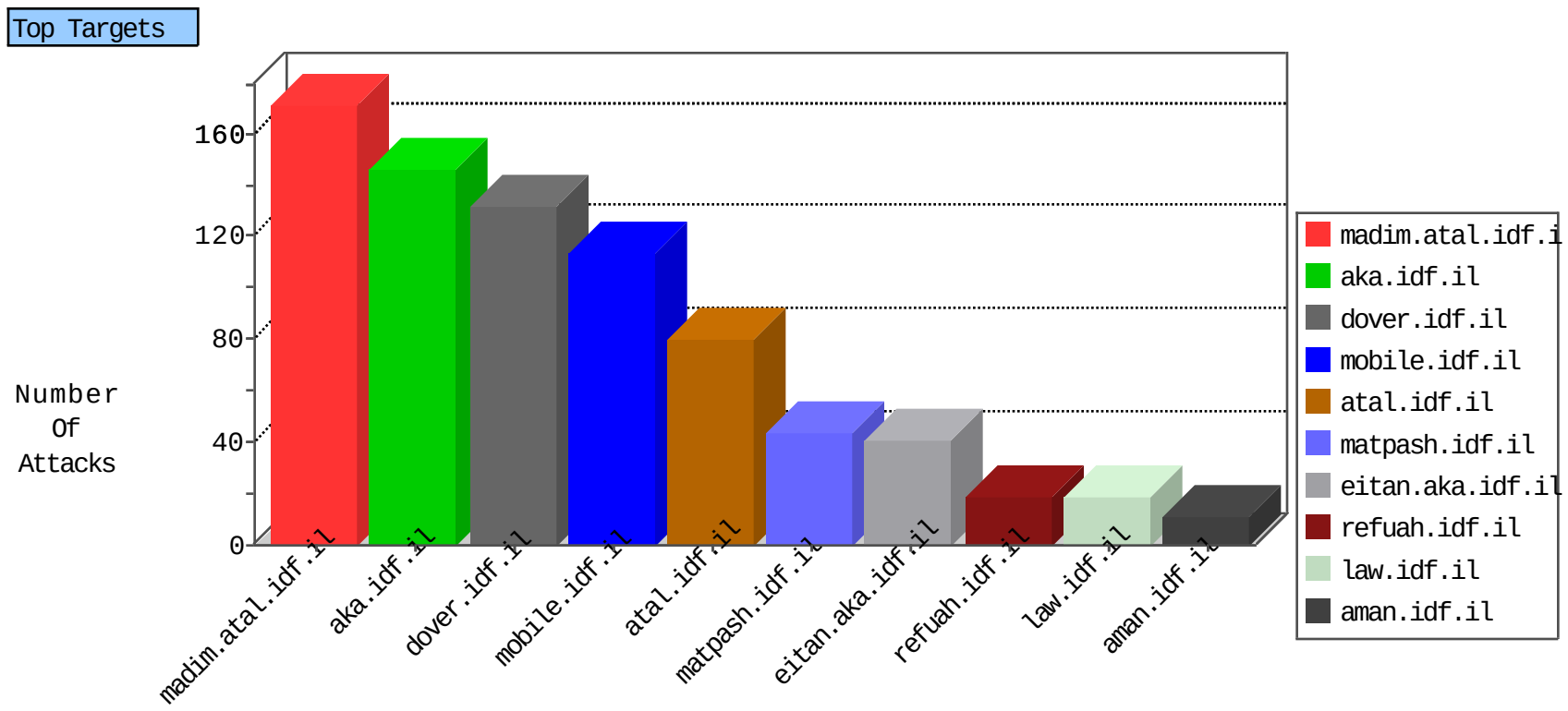
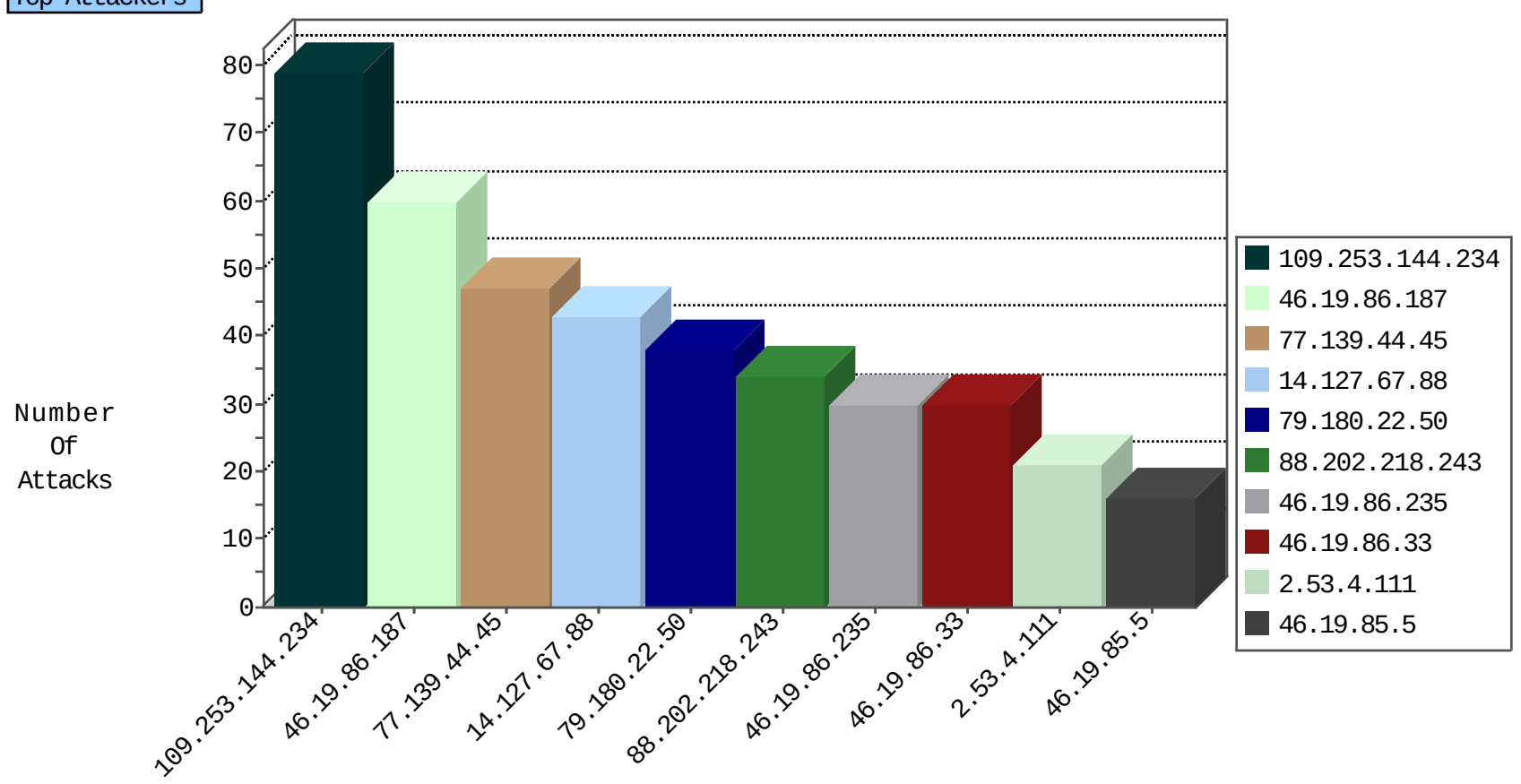
10-01-2016-21:04:09 to 10-01-2016-22:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-01-2016-21:04:09 to 10-01-2016-22:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.230.86.213	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
109.253.214.101	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
141.226.218.49	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
193.37.152.220	Germany	147.237.76.198	e.yohalan.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.94.111.1	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
193.37.152.220	Germany	147.237.76.199	e.nakchal.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.94.111.1	Russian Federation	147.237.76.201	e.atal.idf.il	Black List	drop	1
193.37.152.220	Germany	147.237.76.202	e.halag.idf.il	JLM_Purple_Con_Limit_Http	drop	1
192.69.89.173	United States	147.237.76.30	himush.idf.il	Black List	drop	1

10-01-2016-21:04:09 to 10-01-2016-22:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	1090: HTTP: IIS .asp Source Code Read	Permit	6
125.64.94.206	China	147.237.0.34	tikshuv.idf.il	C1000003: HTTP: phpMyAdmin access	Permit	3
62.212.73.211	Netherlands	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Permit	2
192.187.104.235	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
91.194.84.106	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	1090: HTTP: IIS .asp Source Code Read	Permit	1

10-01-2016-21:04:09 to 10-01-2016-22:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
50.245.143.138	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
41.222.179.6	147.237.0.200	Tanzania, United Republic of	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
77.124.28.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
40.114.15.49	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.66	147.237.76.42	Europe	refuah.idf.il	ET SCAN NMAP -sA (2)	1
40.114.15.49	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.243.100	147.237.77.234	France	halag.idf.il	ET SCAN Potential SSH Scan	1
62.210.243.100	147.237.77.205	France	prisha.idf.il	ET SCAN Potential SSH Scan	1
62.210.243.100	147.237.77.178	France	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.0.33	United Kingdom	idf.il	ET SCAN NMAP -sS window 1024	1
62.210.243.100	147.237.77.74	France	law.idf.il	ET SCAN NMAP -sS window 1024	1
121.223.248.67	147.237.76.42	Australia	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
50.245.143.138	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 4096	1
109.67.176.20	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
41.222.179.6	147.237.72.217	Tanzania, United Republic of	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
77.126.22.145	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
41.215.36.46	147.237.77.234	Kenya	halag.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.152	147.237.77.170	Europe	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
40.114.15.49	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.117	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
62.210.243.100	147.237.77.216	France	dover.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.243.100	147.237.77.179	France	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
202.67.237.220	147.237.76.202	Hong Kong	e.halag.idf.il	ET SCAN Potential SSH Scan	1
62.210.243.100	147.237.77.121	France	e.navy.idf.il	ET SCAN Potential SSH Scan	1
125.64.94.206	147.237.0.34	China	tikshuv.idf.il	GPL WEB_SERVER WEB-MISC JBoss web-console access	1
61.240.144.65	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
117.3.120.166	147.237.0.17	Vietnam	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-01-2016-21:04:09 to 10-01-2016-22:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.187	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
77.139.44.45	France	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
79.180.22.50	Israel	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.53.4.111	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.86.33	Israel	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	18
84.111.64.141	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
46.19.85.5	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
80.246.133.126	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
105.130.245.11	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
87.70.46.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.86.33	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	10
2.53.34.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.158.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
88.202.218.243	United Kingdom	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.253.141.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.139.190.4	France	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
89.139.171.164	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.152.162.74	Netherlands	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.237	Israel	147.237.77.170	maarachot.idf.il	SYN Attack		monitor	4
46.19.85.42	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.213.106	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
176.13.234.203	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
80.246.136.73	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.157	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.125.75.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
80.178.235.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
77.139.44.45	France	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
80.246.136.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.13.249.127	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
37.8.71.190	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
80.246.136.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
85.250.114.206	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.77	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
93.110.21.86	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.111.64.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
93.110.21.86	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.102.6.21	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
84.111.0.114	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.147.164	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
79.178.244.133	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
94.43.247.23	Georgia	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
185.27.105.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.59.208	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.120.122.219	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
5.29.142.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.102.6.21	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
14.127.67.88	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
79.178.244.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2

10-01-2016-21:04:09 to 10-01-2016-22:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.144.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
46.19.86.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
14.127.67.88	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 14.127.67.88	Block	17
88.202.218.243	United Kingdom	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	14
14.127.67.88	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 14.127.67.88	Block	12
79.180.22.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
46.19.86.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
77.138.143.26	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.143.26	Block	6
14.127.67.88	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
141.226.218.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
88.202.218.243	United Kingdom	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1538	Block	5
14.127.67.88	China	147.237.77.74	law.idf.il	PHP Attempt	Block	4
77.138.156.183	France	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	4
88.202.218.243	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
88.202.218.243	United Kingdom	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 88.202.218.243	Block	3
77.139.102.129	France	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	2
2.53.34.173	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.181.122.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	2
195.99.44.54	United Kingdom	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	1
66.249.65.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20581-he/dover.aspx	Block	1
14.127.67.88	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
80.246.133.126	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
77.138.156.163	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.249.65.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9235-he/refuah.aspx	Block	1
157.55.39.100	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.19.86.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalam	Block	1
207.46.13.121	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/contactus/	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
125.64.94.206	China	147.237.0.34	tikshuv.idf.il	Admin Blocking	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	1
37.26.147.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.65.26.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
66.249.66.101	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
14.127.67.88	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/index.asp	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1384-12125-he	Block	1
125.64.94.206	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/docs/	Block	1
77.139.39.241	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
2.53.36.217	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.75.53	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp.	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
66.249.65.139	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8675-he/refuah.aspx	Block	1
141.226.217.240	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
88.202.218.243	United Kingdom	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

10-01-2016-21:04:09 to 10-01-2016-22:04:09