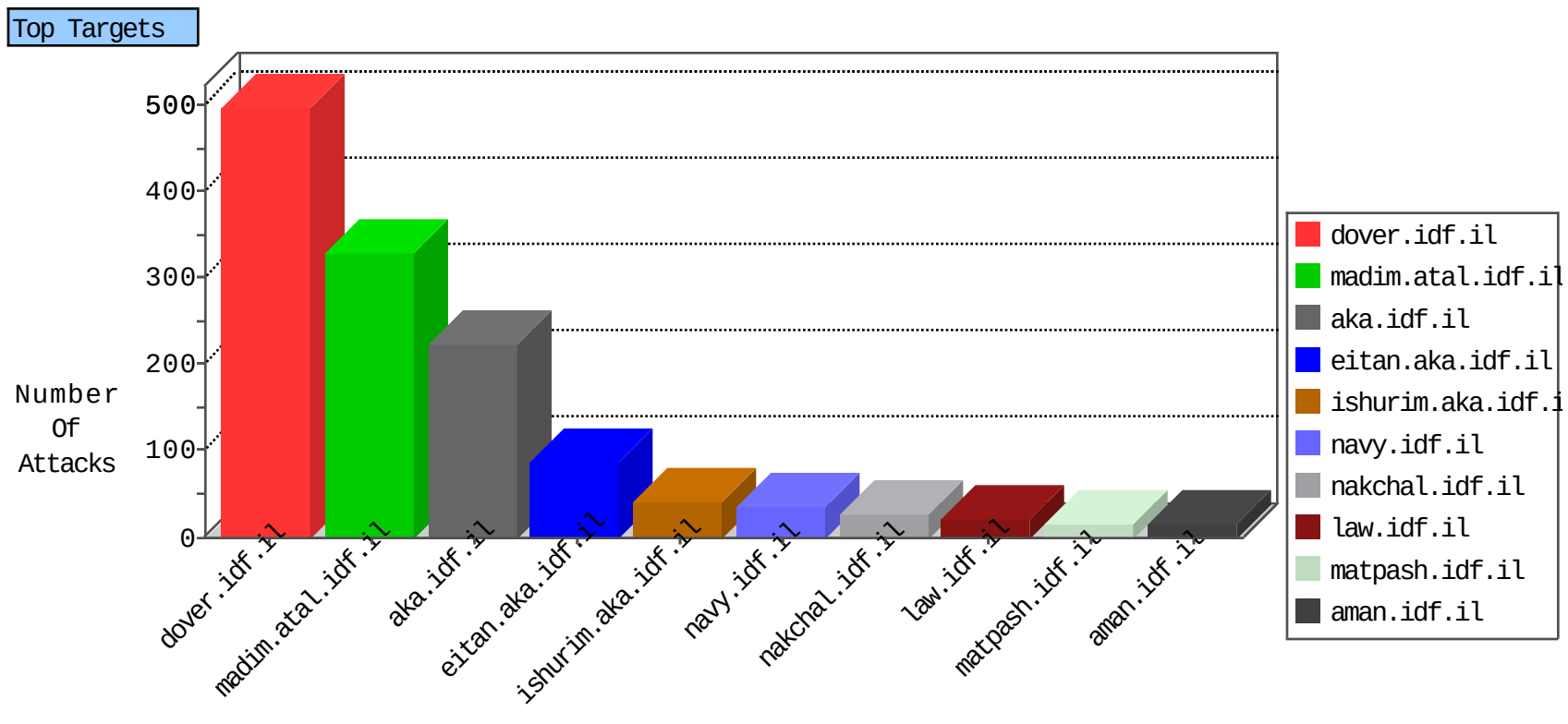
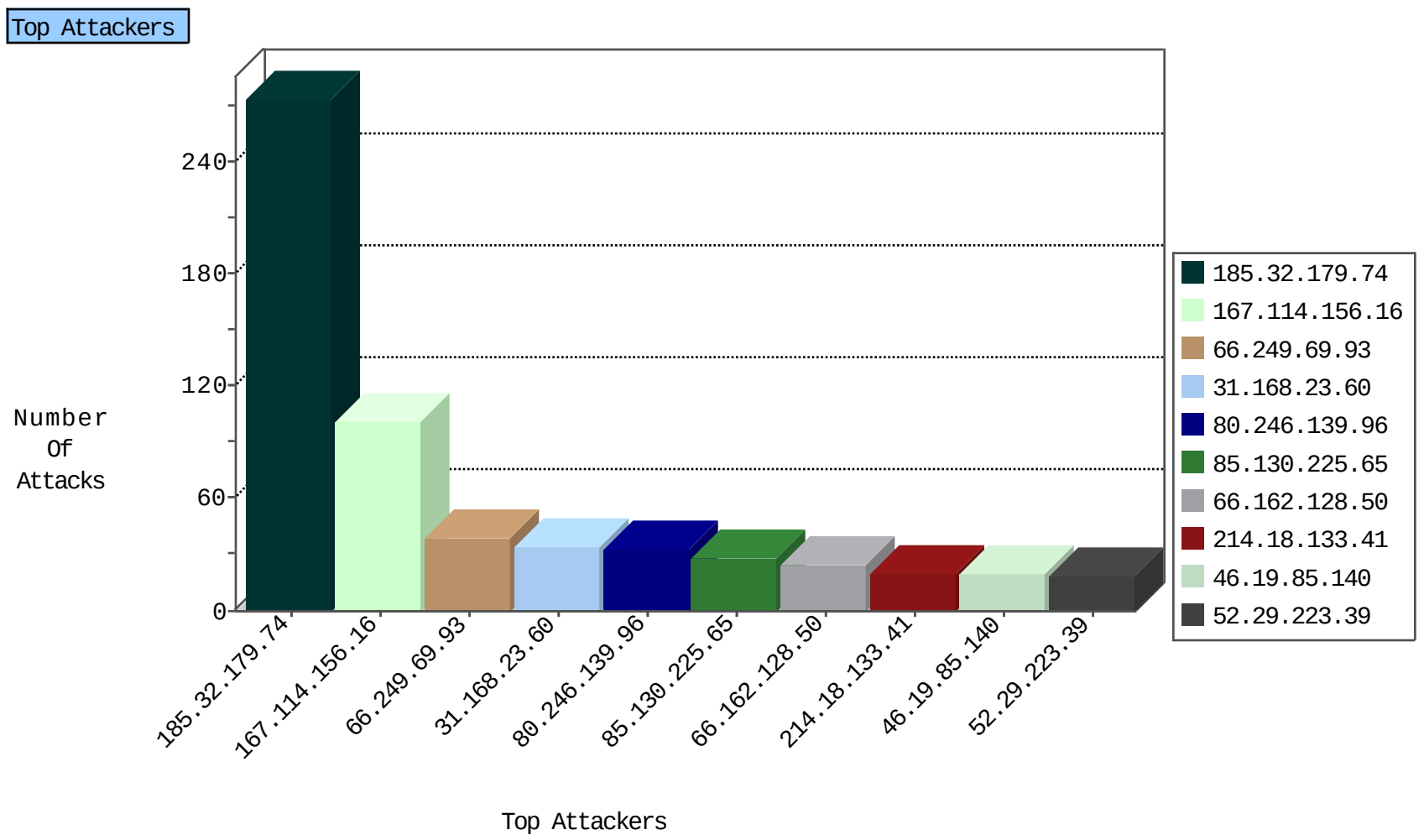
04-20-2016-16:04:08 to 04-20-2016-17:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-20-2016-16:04:08 to 04-20-2016-17:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9306
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	7160
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1019
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	43
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	6
37.26.147.173	Israel	147.237.76.31	nakchal.idf.il	Invalid TCP Flags	drop	6
37.26.147.221	Israel	147.237.76.31	nakchal.idf.il	Invalid TCP Flags	drop	6
81.245.169.187	Belgium	147.237.77.216	dover.idf.il	Invalid L4 Header Length	drop	2
199.203.62.53	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
113.240.250.157	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
142.161.86.202	Canada	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

04-20-2016-16:04:08 to 04-20-2016-17:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-20-2016-16:04:08 to 04-20-2016-17:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
192.198.151.43	147.237.72.167	Europe	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
85.131.208.140	147.237.0.17	Germany	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
84.110.194.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.59.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
46.19.86.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.74	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
13.92.196.2	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.113.132	147.237.76.30	Japan	himush.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
85.131.208.140	147.237.77.19	Germany	law-forum.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.76.177	Germany	ncore.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.8.27	Germany	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.0.16	Germany	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
82.80.73.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
31.210.186.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.39.23	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.130.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.131.208.140	147.237.77.121	Germany	e.navy.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.76.198	Germany	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.76.42	Germany	refuah.idf.il	ET SCAN Potential SSH Scan	1

04-20-2016-16:04:08 to 04-20-2016-17:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
214.18.133.41	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	20
207.241.229.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.162.128.50	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
2.53.175.16	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
188.161.179.212	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	13
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.178.162.82	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.96.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
87.71.115.139	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.64.70	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.185.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.11.230	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.176.97.100	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
198.58.103.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.162.128.50	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
37.142.229.81	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
85.130.225.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.178.158.89	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
85.130.225.65	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.90.131.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
81.218.185.242	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
212.117.136.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.67.164.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.51.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
40.77.167.64	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.140	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
5.102.195.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.140	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.178.158.89	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.102.9.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.46.41.255	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.109.230.97	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.130.225.65	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.53.48.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
100.34.86.83	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.30.24.125	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.102.9.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
88.254.109.108	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.102.195.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	273
80.246.139.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
2.53.52.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
46.19.86.249	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
66.102.6.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
213.57.251.102	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/7/	Block	3
78.34.82.178	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	3
46.120.120.217	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.120.217	Block	3
176.13.19.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.20.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.82.65.82	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	2
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/shared/clientscripts/scroller/jquery.jcarousel.js	None	1
66.249.75.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/shared/clientscripts/jquery.plugins/jquery.equalheights.js	None	1
204.79.180.128	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.7.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
46.19.86.93	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/mobile	Block	1
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/style/shared/960.css	None	1
87.71.94.241	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/shared/clientscripts/jquery/jquery-1.4.2.min.js	None	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
79.180.28.1	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl57 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.120.120.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/g	Block	1
31.168.23.60	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.23.60	Block	1
106.186.113.132	Japan	147.237.76.30	himush.idf.il	Multiple Untraceable SSL Sessions from 106.186.113.132 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
82.80.143.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/shared/clientscripts/sidebar/sidebar.js	None	1
207.46.13.56	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.75.26	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/shared/clientscripts/jquery.plugins/jquery.scrollfollow.js	None	1
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/style/shared/datepicker.css	None	1
105.103.15.225	Algeria	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/shared/clientscripts/jquery/jquery-ui.js	None	1
213.57.160.201	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/site/spotting/spotting.asp	Block	1
79.181.220.132	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
66.102.6.188	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.55.50.3	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
192.115.130.253	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/112251.pdf	Block	1
106.186.113.132	Japan	147.237.76.30	himush.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
37.26.146.166	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
84.94.114.184	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/shared/clientscripts/ui/i18n/jquery-ui-i18n.js	None	1
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/shared/clientscripts/jquery.plugins/slider.js	None	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/gallery.aspx	Block	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
46.120.18.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/style/shared/layout2.css	None	1
105.103.15.225	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.103.15.225	Block	1
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/shared/clientscripts/jquery/jquery.nyromodal-1.6.2.js	None	1
213.57.251.102	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/sip_storage/files/7	Block	1