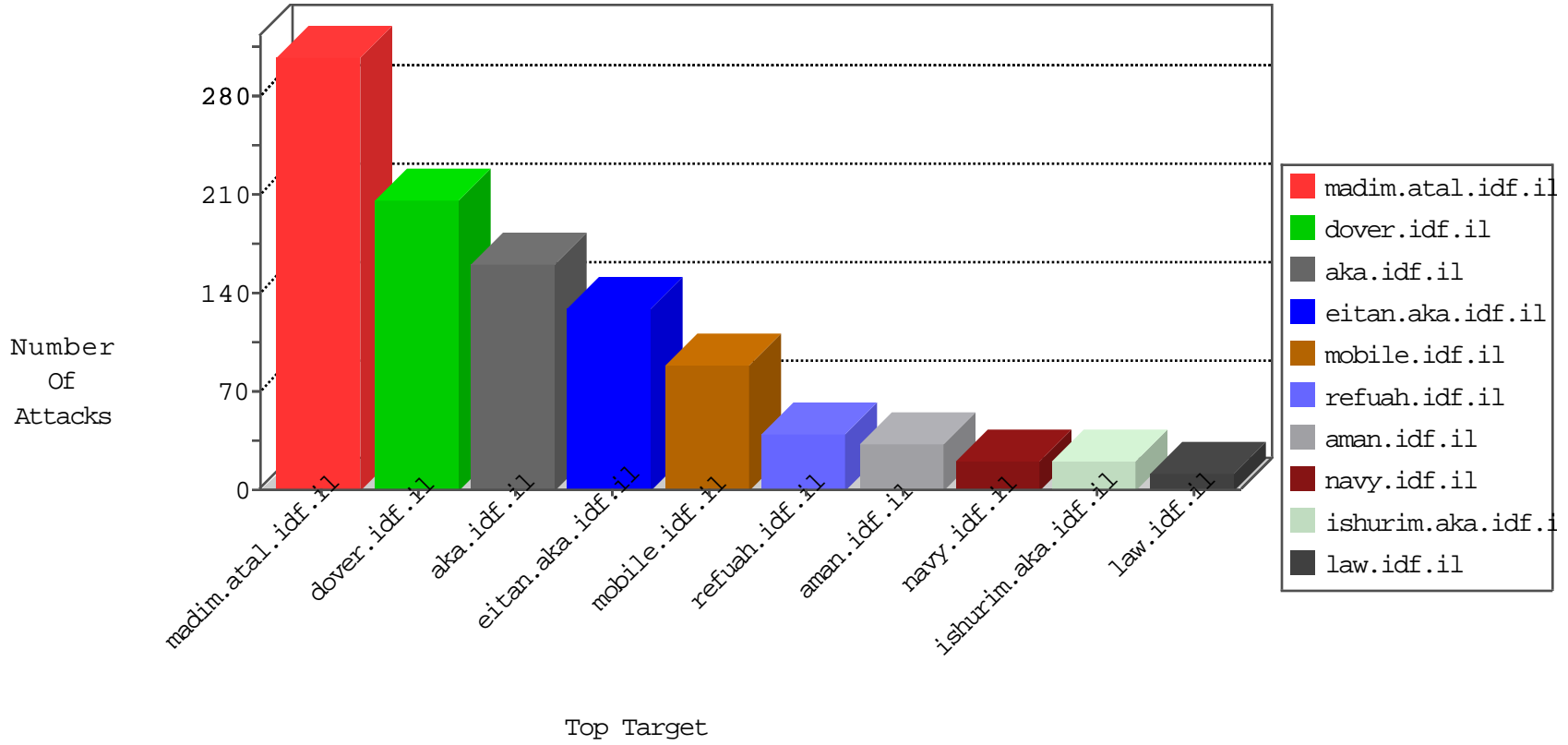


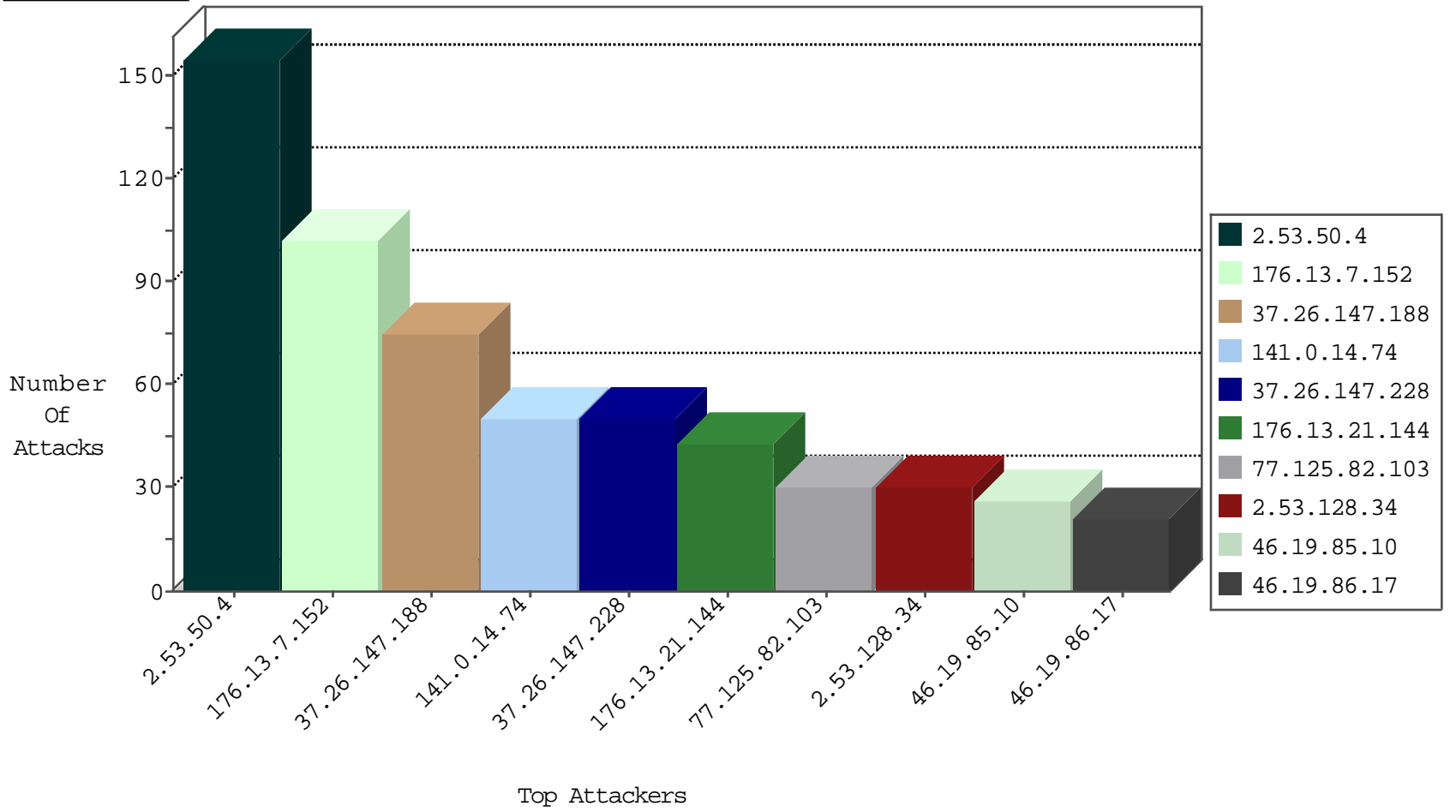
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.22.244	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
10.0.0.4		147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	5
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
79.181.241.30	Israel	147.237.77.226	www.chamatz.aka.idf.il	Black List	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
85.64.61.134	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
192.33.90.68	Switzerland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
156.56.250.226	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-15-2016-18:04:08 to 09-15-2016-19:04:08

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
175.207.77.148	147.237.77.74	Korea, Republic of	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	3
47.88.5.234	147.237.72.156	Canada	aman.idf.il	ET SCAN Potential SSH Scan	1
191.235.92.192	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.76.199	Japan	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.54.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
133.208.21.66	147.237.0.200	Japan	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
109.60.153.178	147.237.8.45	Russian Federation	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.155	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
202.155.58.28	147.237.76.86	Indonesia	navy.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
192.81.216.190	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
47.88.5.234	147.237.77.234	Canada	halag.idf.il	ET SCAN Potential SSH Scan	1
191.235.92.192	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.158	147.237.76.197	Sweden	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
191.235.92.192	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
42.112.27.123	147.237.0.17	Vietnam	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
133.242.4.52	147.237.76.198	Japan	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
2.55.146.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
133.208.21.66	147.237.76.38	Japan	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
123.136.27.66	147.237.0.17	Bangladesh	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.8.24	Russian Federation	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.155	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
202.155.58.28	147.237.72.14	Indonesia	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
66.212.179.106	147.237.0.15	Canada	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
191.235.92.192	147.237.77.212	United States	e.dover.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.147.188	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
141.0.14.74	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
37.26.147.228	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.53.128.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
77.125.82.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
109.67.124.27	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.86.17	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
37.26.147.228	Israel	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
2.53.22.144	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
193.106.52.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.229.152.110	United Kingdom	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.120.173.58	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
37.26.147.228	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.17	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
78.168.65.10	Turkey	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
176.228.133.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
37.26.148.218	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.53.63.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.53.128.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.114	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
84.95.133.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.214.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
84.108.11.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
79.179.215.244	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
156.198.131.34	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
188.120.154.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.113	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.64.124	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.82.6	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.134.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.22.105	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.17	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
66.249.69.89	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.240.53	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	3
207.46.13.95	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.140	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.182.113.179	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.17	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.66.6.88	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.150.155	Israel	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
84.108.11.190	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
79.177.190.49	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.50.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	155
176.13.7.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
176.13.21.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
109.253.159.49	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.253.159.49	Block	4
79.179.154.135	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	4
87.14.140.14	Italy	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	4
185.32.179.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.233.11	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx	Block	2
47.150.103.202	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	2
109.253.159.49	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	2
176.13.228.207	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.228.207	Block	2
79.114.140.196	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	2
176.13.228.207	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
46.19.85.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.176.75	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.86.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.9.47	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
66.249.76.20	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
46.102.98.197	Estonia	147.237.76.147	chinuch.aka.idf.il	PHP Attempt	Block	1
89.237.76.113	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
207.46.13.110	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
46.19.85.38	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.181.133.176	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
75.82.100.127	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/	Block	1
46.102.98.197	Estonia	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/wp-login.php	Block	1
2.53.14.19	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
93.172.147.208	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.102.9.2	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
213.57.45.8	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
46.19.85.103	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	1
77.138.88.179	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunpersonalquestionnaire.aspx	Block	1
46.116.17.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
106.184.21.147	Japan	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
79.177.190.49	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1400-he/atal.aspx	Block	1
131.253.25.128	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.aspx/getjs	Block	1
84.110.48.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
77.138.153.25	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
46.117.30.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.64.91.100	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$emailUpdate\$hiddenUpdateEmail in www.aka.idf.il/main/giyus/faq.aspx	None	1
66.249.66.29	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1399-he/atal.aspx	Block	1
77.138.234.231	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
46.120.137.255	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus	Block	1
192.115.190.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.50.144	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
5.29.124.129	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1