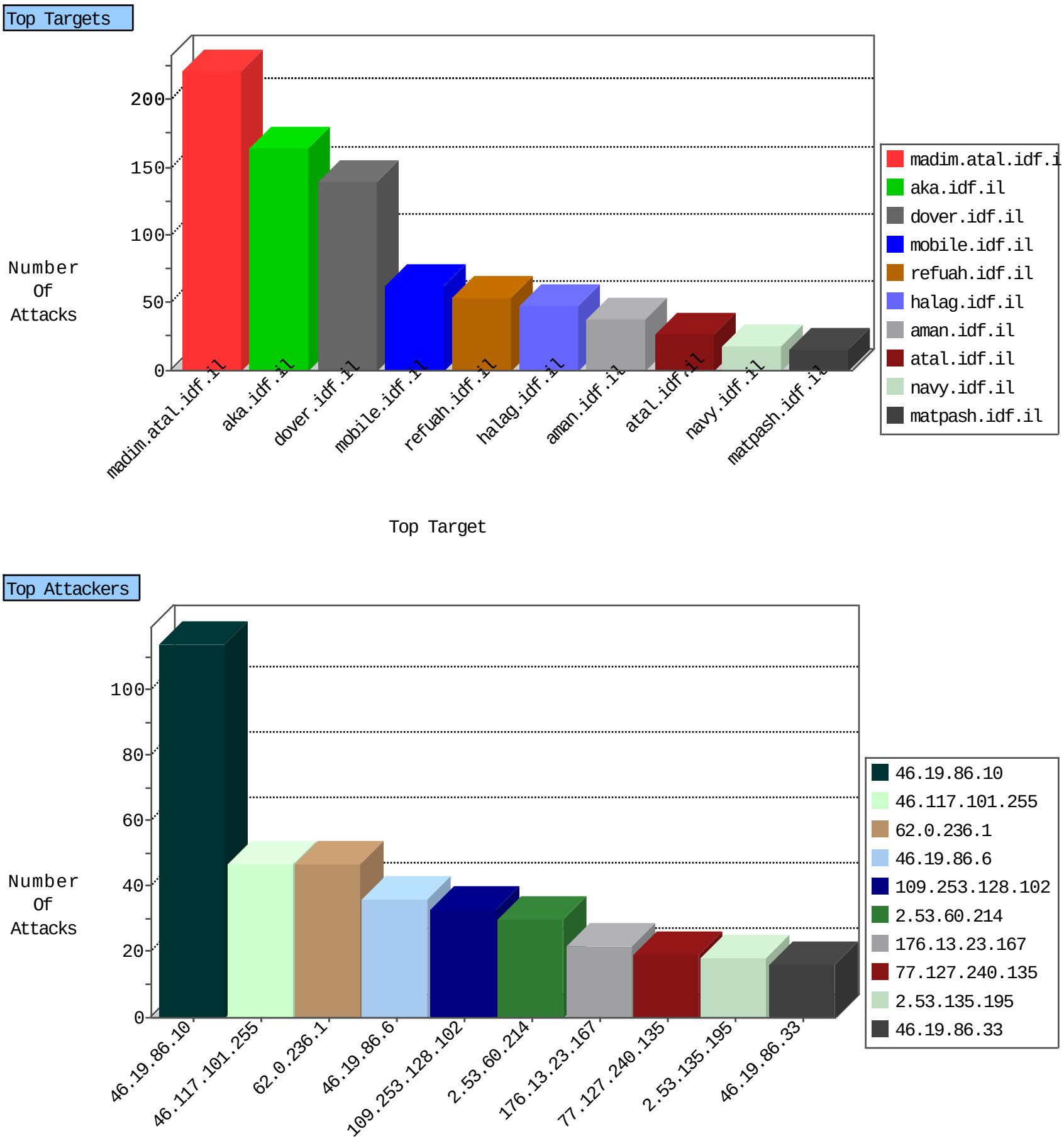
09-15-2016-08:04:05 to 09-15-2016-09:04:05

IDF Under Attack Daily Report



09-15-2016-08:04:05 to 09-15-2016-09:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.38.29	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.34	Germany	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
70.28.55.106	Canada	147.237.77.121	e.navy.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-15-2016-08:04:05 to 09-15-2016-09:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.149.126.98	Germany	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-15-2016-08:04:05 to 09-15-2016-09:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.143.168.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
62.215.38.173	147.237.77.212	Kuwait	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
202.79.60.94	147.237.8.50	Nepal	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
62.128.45.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
200.98.129.125	147.237.76.44	Brazil	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
62.0.102.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.23.181.171	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.203.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.217.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
221.210.200.245	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
62.219.35.77	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.215.38.173	147.237.77.212	Kuwait	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
201.132.203.154	147.237.0.35	Mexico	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
62.90.202.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.62.18.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.227.67.158	147.237.0.200	Sweden	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
42.116.29.68	147.237.76.176	Vietnam	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
108.185.177.89	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
94.102.48.195	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
87.69.66.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
221.210.200.245	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
77.124.3.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.227.55.94	147.237.76.30	Germany	himush.idf.il	ET SCAN Potential SSH Scan	1

09-15-2016-08:04:05 to 09-15-2016-09:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.117.101.255	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	46
62.0.236.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	43
2.53.60.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.53.135.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.149.158	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
46.19.86.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
37.26.149.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
87.68.36.107	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
80.178.89.27	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.33	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.86.6	Israel	147.237.77.216	dover.idf.il	SYN Attack		monitor	7
176.13.17.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.164	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.33	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
77.127.240.135	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.164	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.127	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.244.139	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.6	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
212.179.218.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.179.218.166	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.127.240.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.253.145.151	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.220	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
109.253.210.182	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
132.74.113.132	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
212.179.218.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.64.84.152	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.236.112	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
185.32.179.125	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.78	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
93.104.215.125	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
77.127.240.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.78	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
94.230.86.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack		monitor	3
46.19.85.117	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.200	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
146.196.36.122		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.152	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.96	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

09-15-2016-08:04:05 to 09-15-2016-09:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	114
109.253.128.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
176.13.23.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
2.53.188.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
46.19.86.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
37.26.148.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
80.246.136.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.210.205.51	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	3
109.253.205.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
86.246.8.24	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
46.19.85.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/areceber	Block	2
37.26.148.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.50.144	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
176.13.246.160	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.137	Block	1
46.232.130.154	Poland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunlobby.aspx	Block	1
207.46.13.57	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
157.55.39.227	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/links/links.aspx	Block	1
77.138.94.241	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/apple-app-site-association	Block	1
185.32.179.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.55.133.158	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.155.176	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 109.67.155.176	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/apple-app-site-association	Block	1
65.49.68.201	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/8/	Block	1
165.225.80.105	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	Block	1
80.178.89.27	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
2.53.14.185	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
192.114.5.10	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
46.116.103.204	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
37.26.147.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.155.176	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.aspx	Block	1
66.102.7.136	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
46.19.85.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.50.144	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.45	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/edim/yoman/yoman.asp	Block	1
192.114.5.10	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.117.101.255	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.66.15	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
176.13.23.167	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
66.249.64.134	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/assetlinks.json	Block	1
204.79.180.155	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
68.180.230.225	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/showpicture.asp	Block	1

09-15-2016-08:04:05 to 09-15-2016-09:04:05