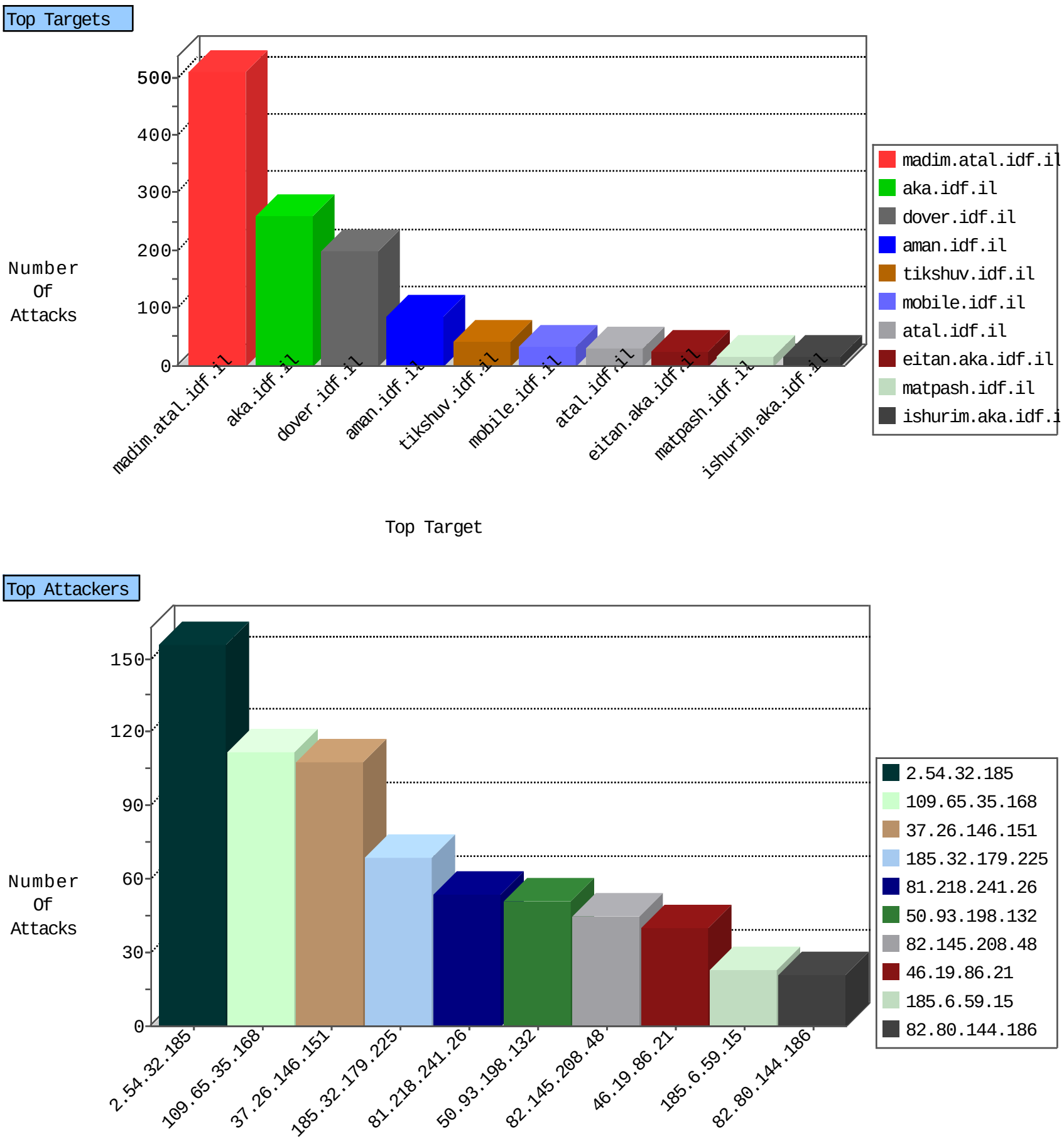
03-09-2016-21:04:04 to 03-09-2016-22:04:04

IDF Under Attack Daily Report



03-09-2016-21:04:04 to 03-09-2016-22:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	218
82.145.208.48	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	45
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
185.94.111.1		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
82.221.105.6	Iceland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
188.138.17.205	France	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.206	Netherlands	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
31.28.170.110	Ukraine	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
113.190.0.94	Vietnam	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

03-09-2016-21:04:04 to 03-09-2016-22:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.141.99	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	6
109.65.143.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
81.218.251.251	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
123.126.113.163	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
213.57.197.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
212.251.221.118	Norway	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
212.251.221.118	Norway	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
10.0.0.8		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
207.46.13.98	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-09-2016-21:04:04 to 03-09-2016-22:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
37.26.146.151	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
122.147.148.178	147.237.77.170	Taiwan	maarachot.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
79.176.80.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.142.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.62.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
161.10.217.207	147.237.76.30	Colombia	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.193	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.158	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
192.116.166.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-09-2016-21:04:04 to 03-09-2016-22:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.218.241.26	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	28
82.80.144.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
5.22.130.79	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
185.6.59.15	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
166.170.30.190	United States	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
188.120.154.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
185.6.59.15	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
176.13.4.152	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
87.71.144.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.4.152	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
62.219.137.5	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
84.228.237.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.184.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.149.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.5.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.39.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.148.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.93.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
208.89.33.29		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.229.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.228.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.229.94	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.108.181.56	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.25.231.237	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
206.74.42.69	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.228.10.204	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
132.66.235.218	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.102.195.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
132.66.235.218	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.26.146.151	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		alert	4
5.22.135.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
217.132.116.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.151	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	4
79.183.189.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.0.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.242.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
147.235.8.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
212.199.250.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.157.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.109.206.19	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.52.32.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.114.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
75.150.130.217	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
132.66.235.218	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
37.142.184.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.180.173.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
147.235.8.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
178.95.248.23	Ukraine	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.32.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	156
109.65.35.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
37.26.146.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
185.32.179.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
46.19.86.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
84.110.38.110	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	9
46.19.85.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
50.93.198.132	United States	147.237.0.15	kosher-kravi.idf.il	Distributed PHP Attempt	Block	4
50.93.198.132	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 50.93.198.132	Block	4
50.93.198.132	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
50.93.198.132	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
2.54.174.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
50.93.198.132	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 50.93.198.132	Block	3
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.183.235	Block	3
50.93.198.132	United States	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	2
50.93.198.132	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 50.93.198.132	Block	2
50.93.198.132	United States	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 50.93.198.132	Block	2
50.93.198.132	United States	147.237.76.86	navy.idf.il	PHP Attempt	Block	2
108.205.37.40	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
50.93.198.132	United States	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	2
50.93.198.132	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 50.93.198.132	Block	2
50.93.198.132	United States	147.237.72.156	aman.idf.il	PHP Attempt	Block	2
109.64.22.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
50.93.198.132	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 50.93.198.132	Block	2
176.13.7.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.151	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
50.93.198.132	United States	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	2
50.93.198.132	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 50.93.198.132	Block	2
176.13.18.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
50.93.198.132	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
50.93.198.132	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	2
50.93.198.132	United States	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 50.93.198.132	Block	2
65.55.210.198	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1
27.19.144.25	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
50.93.198.132	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 50.93.198.132	Block	1
50.93.198.132	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 50.93.198.132	Block	1
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/sachar/	Block	1
46.120.129.109	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
77.66.90.166	Denmark	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/blog/wp-admin/	Block	1
37.99.14.118	Kazakstan	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/	Block	1
204.79.180.235	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.65.149.140	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/login	Block	1
84.111.39.77	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
186.214.133.204	Brazil	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
50.93.198.132	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
79.178.51.223	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
37.142.64.50	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1