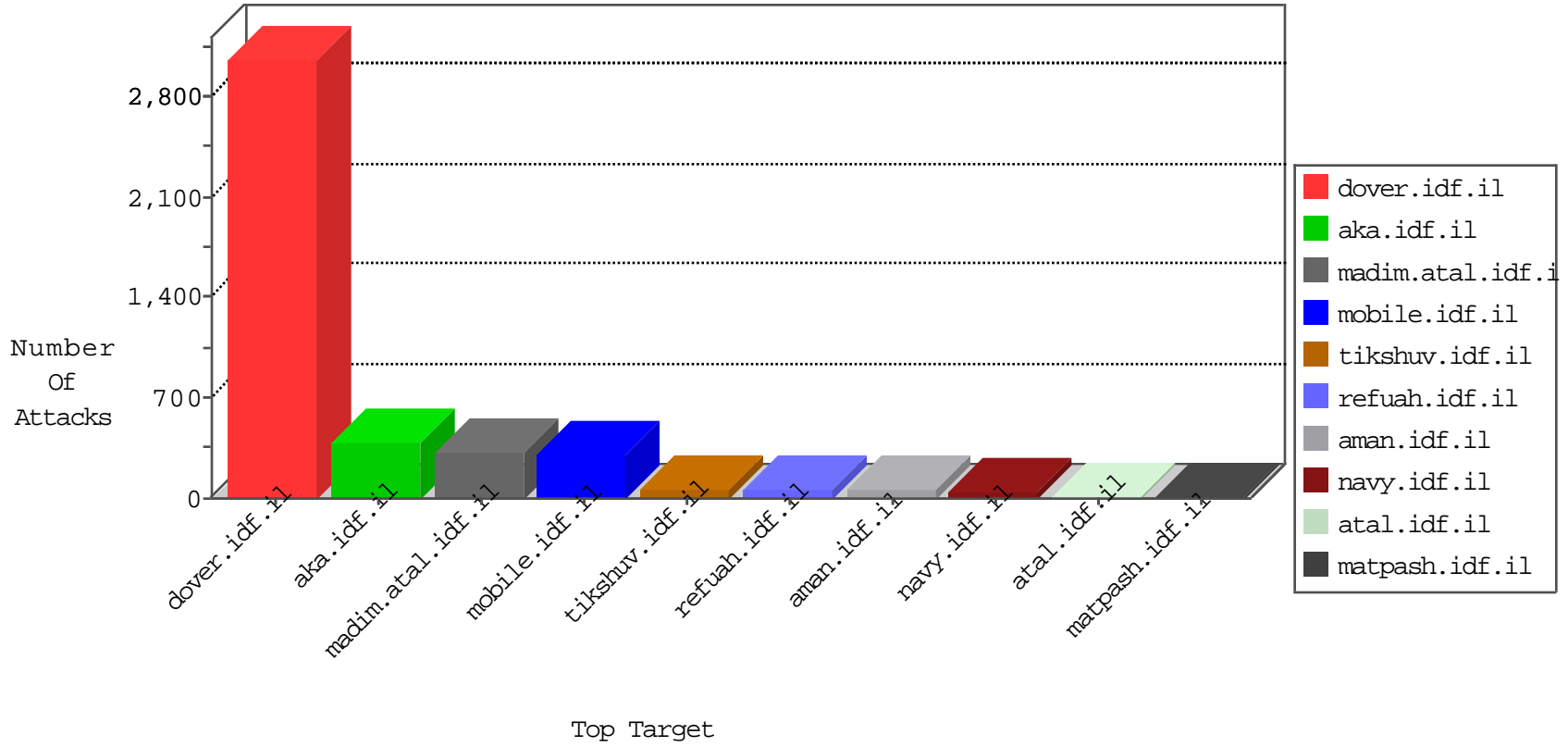


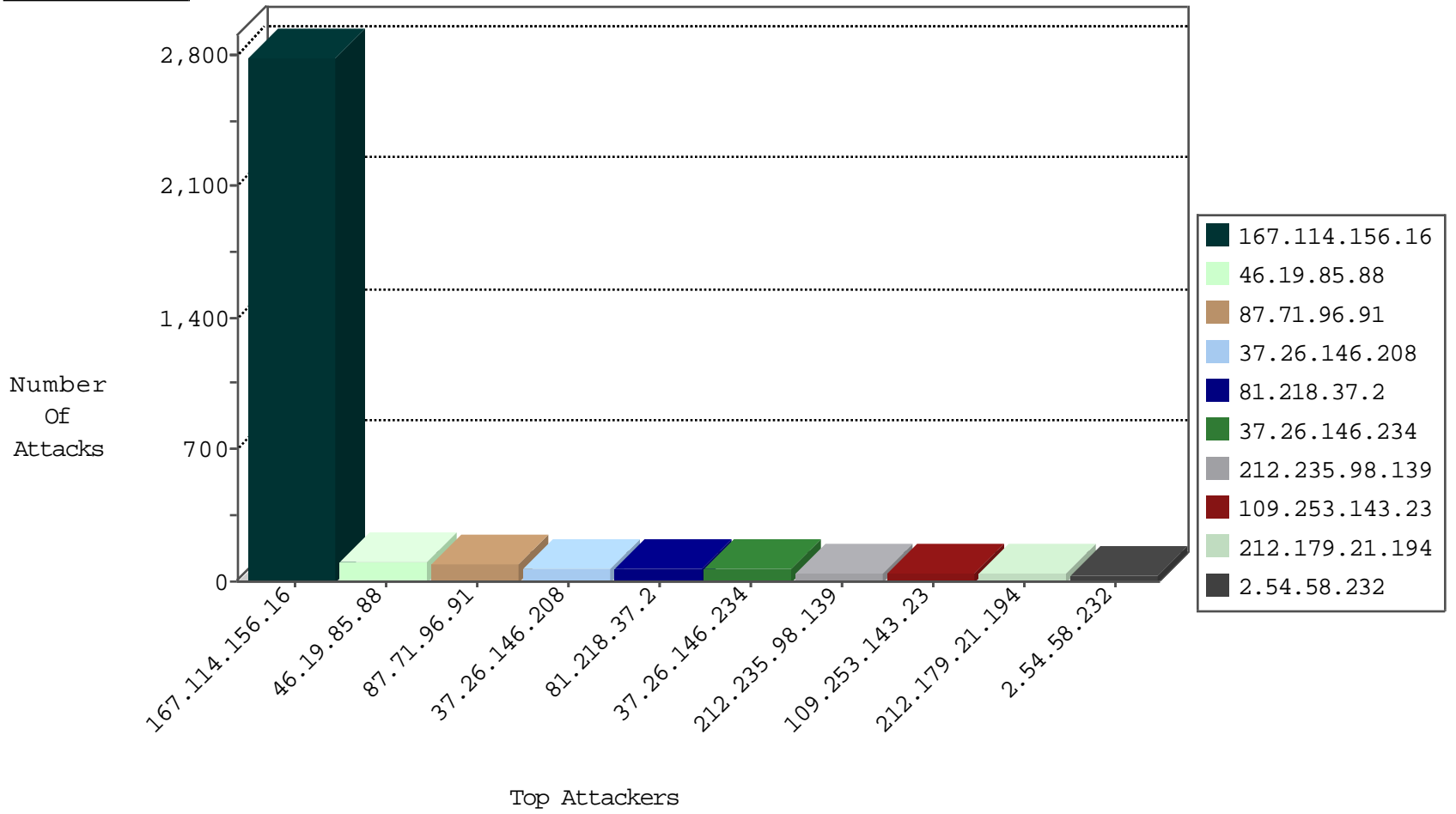
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3565
81.218.37.2	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	288
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
77.126.144.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
212.235.98.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
212.143.191.195	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
82.145.209.18	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
67.211.220.26	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
84.108.57.175	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
79.177.103.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
31.171.155.29	Albania	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.23	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
79.182.98.136	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
62.210.115.133	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	8
79.183.160.119	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
5.29.127.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
79.178.161.161	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.179.179.1	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
212.143.3.162	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
212.199.205.68	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
85.64.249.42	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.24.142	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.59.60.67	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
62.210.115.133	France	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.69.26	147.237.77.216	United States	dover.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	2
79.178.236.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.161.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
213.8.204.56	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.215	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.72.14	United States	dover.idf.il(olc	ET DROP Dshield Block Listed Source	1
2.54.178.41	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.6.0	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.48.37	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.114	147.237.76.86	Ukraine	navy.idf.il	ET SCAN NMAP -sS window 1024	1
82.81.70.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.3.96	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.175.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.72.179.221	147.237.77.243		mobile.idf.il	ET SCAN NMAP -sS window 1024	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
110.35.204.39	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.114	147.237.76.86	Ukraine	navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	90
87.71.96.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
37.26.146.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	40
109.253.143.23	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	30
81.218.37.2	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
176.13.10.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
77.87.228.68	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.85.153	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
212.179.21.194	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
2.54.167.111	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
81.218.241.26	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	14
66.249.66.18	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.137.207	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.81.46.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
81.218.37.2	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
109.253.137.240	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.3.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.105	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
176.13.10.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.146.189	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.219.137.5	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.36.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.163.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.144.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.3.144.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.235.98.139	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
77.126.144.139	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.64.109.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.141	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.105	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.71.111.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.164.86	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.7	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.229	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.148.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.153	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
5.102.242.224	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
37.26.146.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
2.54.58.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
37.26.146.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
2.54.27.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
37.26.146.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
87.71.96.91	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	16
2.54.58.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
37.26.146.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
37.26.146.208	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
109.253.143.23	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
87.71.58.141	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.71.58.141	Block	8
46.19.86.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
5.22.130.72	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 5.22.130.72	Block	4
2.54.137.207	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.120.131.155	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.120.131.155	Block	4
80.246.136.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.16.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.137.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.198	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	3
37.26.146.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.120.131.155	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
46.19.86.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.71.58.141	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/giyus/general.aspx	Block	2
109.253.137.240	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.146.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.34	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
208.115.113.84	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/1/1381.pdf	Block	1
5.22.130.78	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
109.253.133.61	Israel	147.237.77.234	halag.idf.il	Parameter Type Violation SearchText in www.logistics.atal.idf.il/938-he/halag.aspx	Block	1
93.172.165.26	Israel	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 93.172.165.26	Block	1
46.19.85.225	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Header Name ifqúly[#26]]>óvKLÁwS¿[[#5]]dpé[[#17]]K[[#23]]@	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Malformed URL	Block	1
37.26.148.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.49	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
66.249.66.15	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
176.13.8.125	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.54.184.24	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
95.135.254.246	Ukraine	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
68.180.230.189	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
37.26.146.234	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
46.121.232.50	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1