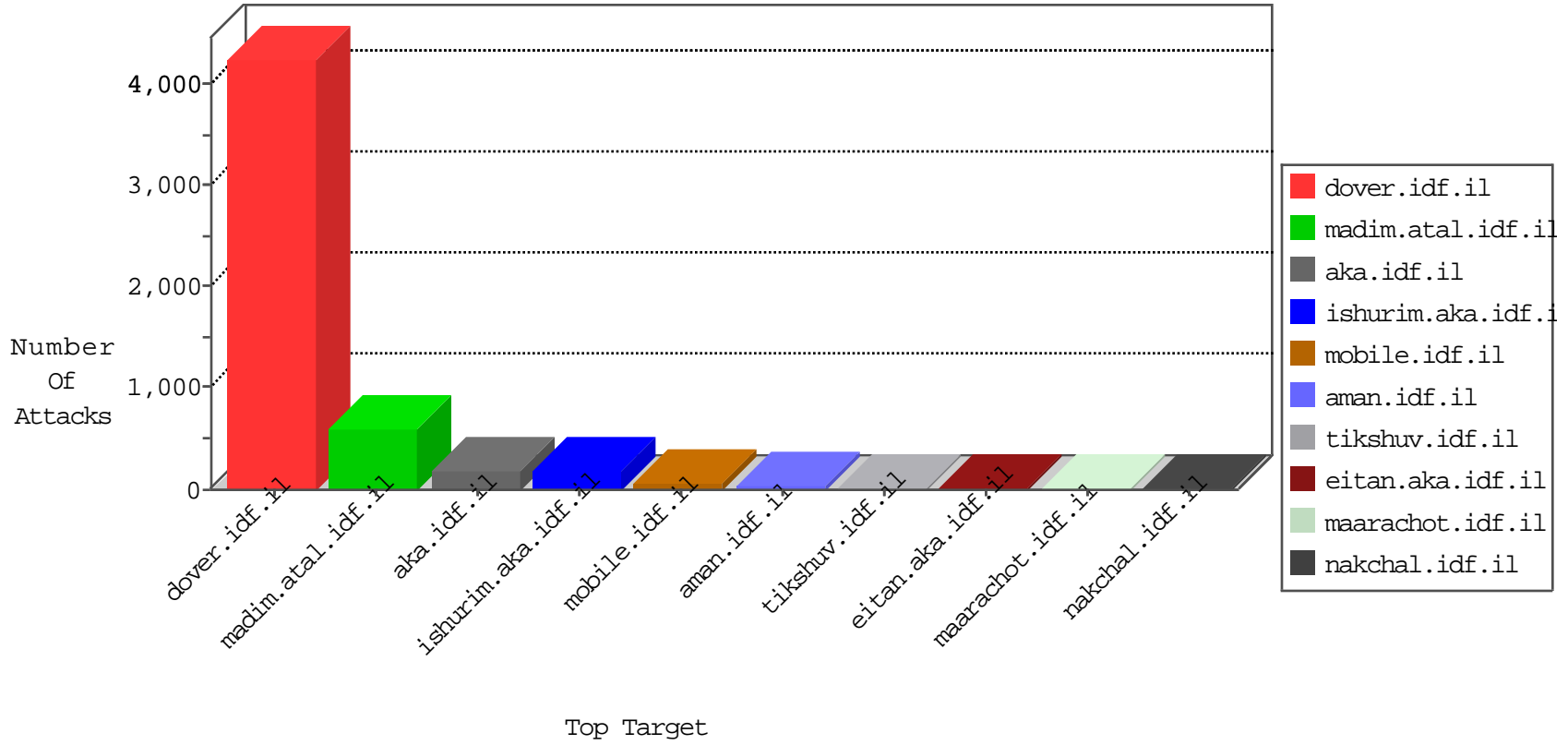


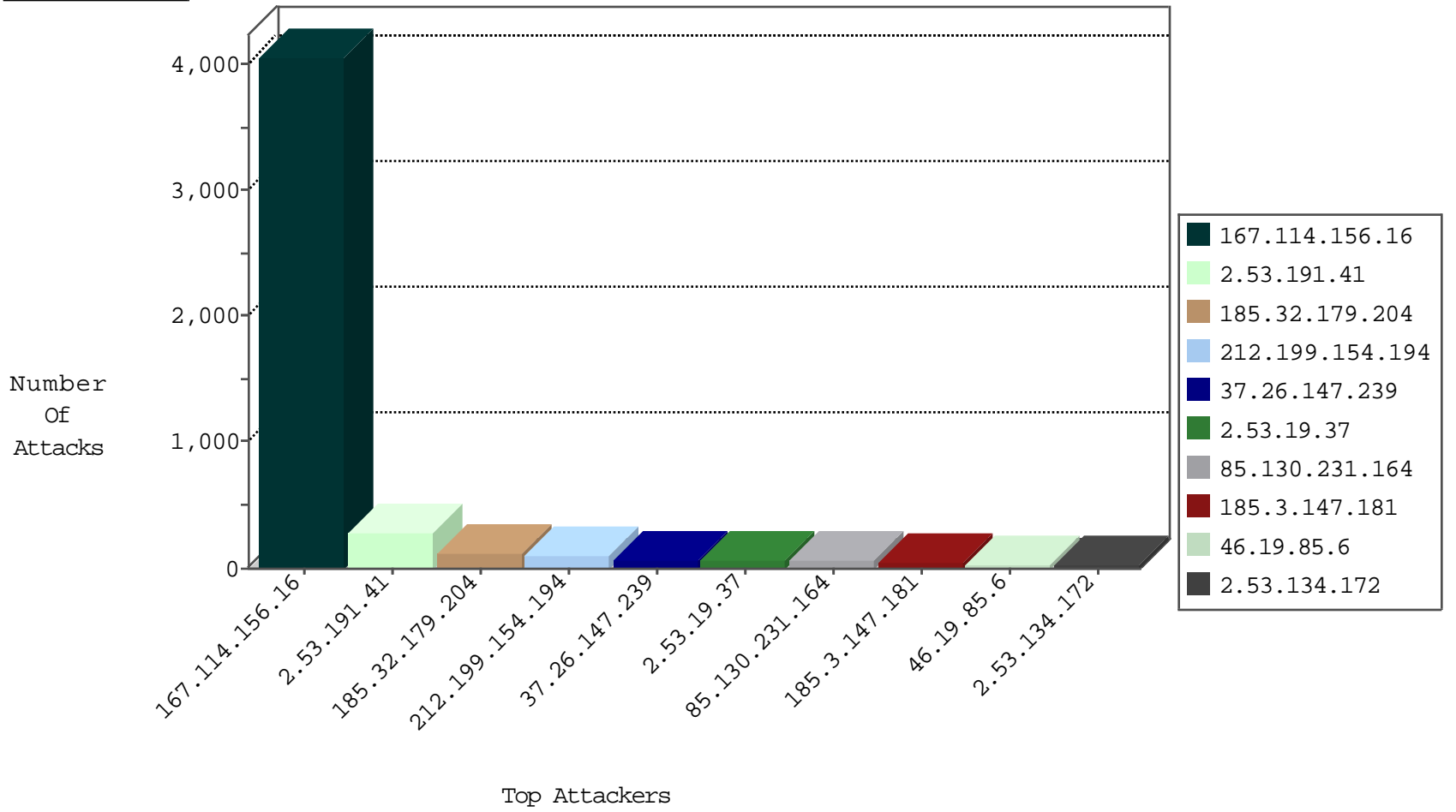
IDF Under Attack Daily Report



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	Block_Ip_Web_In	drop	4046
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	548
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
58.234.85.208	Korea, Republic of	147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	2
184.105.139.105	United States	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	1
113.240.250.157	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
45.32.231.87	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
46.19.85.163	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-19-2016-12:04:00 to 04-19-2016-13:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.187.114.11	United States	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	2

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
125.212.232.165	147.237.77.235	Vietnam	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
111.13.70.132	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
80.246.139.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.117.136.108	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
14.161.36.92	147.237.0.33	Vietnam	idf.il	ET SCAN NMAP -sS window 1024	1
210.140.73.42	147.237.77.216	Japan	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.21.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
146.185.60.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
120.194.193.15	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.214.149.209	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.39	Netherlands	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
46.19.86.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.25.79.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
190.141.150.40	147.237.0.35	Panama	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
176.13.2.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.130.231.164	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	35
37.26.147.239	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
2.53.30.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.53.140.81	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
147.236.238.83	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.211.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.235.34.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.147.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.147.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
37.26.147.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.166.101	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.26.147.239	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
147.236.38.29	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
37.26.147.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
37.26.147.239	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
109.64.207.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.19.37	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.151.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.131.244	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.116.6.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.97	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.147.239	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.55.187.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.116.6.160	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.20	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.105	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.2.227	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.242.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.177.96.161	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.55.24.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.215.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.93.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
193.37.129.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.130.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.49.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.183.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.12.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.113.137	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	3
212.68.144.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.184.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-19-2016-12:04:00 to 04-19-2016-13:04:00

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.55.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.106.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.191.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	287
185.32.179.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
2.53.19.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
185.3.147.181	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 185.3.147.181	Block	32
46.19.85.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
2.53.134.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
109.253.227.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
46.19.86.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
2.55.179.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
2.53.131.244	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Email in mobile.idf.il/sachar/createaccount	Block	8
193.222.161.6	Switzerland	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/0/	Block	6
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.56.171	Block	5
37.46.39.193	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	4
2.55.24.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatgquantity.aspx	Block	3
2.53.181.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
147.236.38.29	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	3
37.26.147.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.12.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.22.239	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.53.22.239	Block	3
37.46.39.193	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.46.39.193	Block	3
80.246.136.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.138.181.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
2.53.22.239	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
2.53.160.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.227.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
193.222.161.6	Switzerland	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/	Block	2
31.168.125.0	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
80.246.130.163	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
179.36.193.101	Argentina	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 179.36.193.101	Block	2
185.32.179.216	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.117.140.170	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
179.36.193.101	Argentina	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	2
212.117.140.170	Israel	147.237.72.166	aka.idf.il	Distributed Unknown Parameter on www.aka.idf.il/main/kapatz/scriptresource.axd parameter amp;t	None	1
79.181.155.221	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/contactus/mobile	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16311-	Block	1
54.193.14.136	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
213.171.218.193	United Kingdom	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/test/wp-admin/	Block	1
95.86.99.148	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
80.246.139.114	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.174	Block	1
157.55.39.76	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.116.6.160	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
89.138.193.120	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	1
2.53.63.167	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
185.3.147.181	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
80.246.130.84	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.193.14.136	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/wp-login.php	Block	1