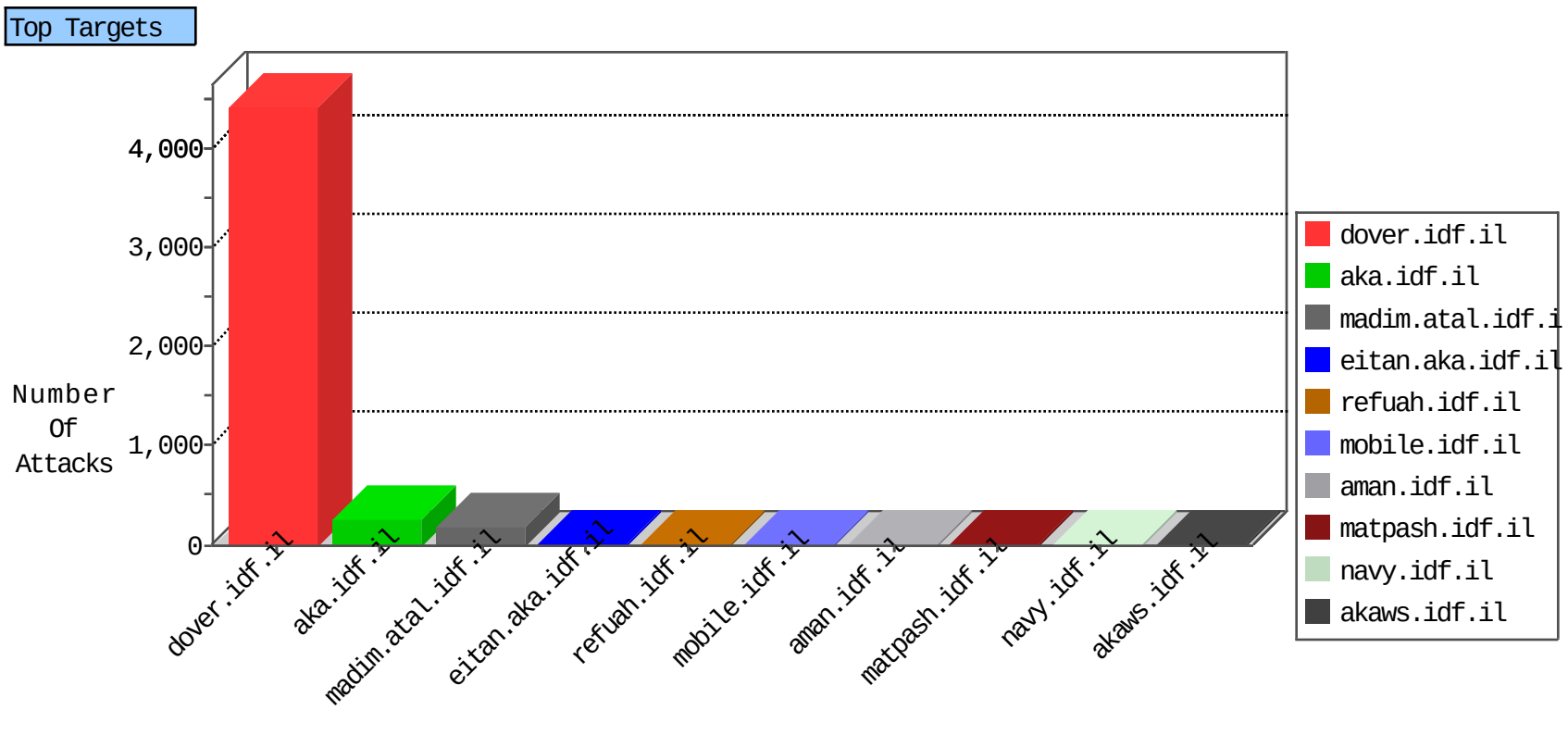
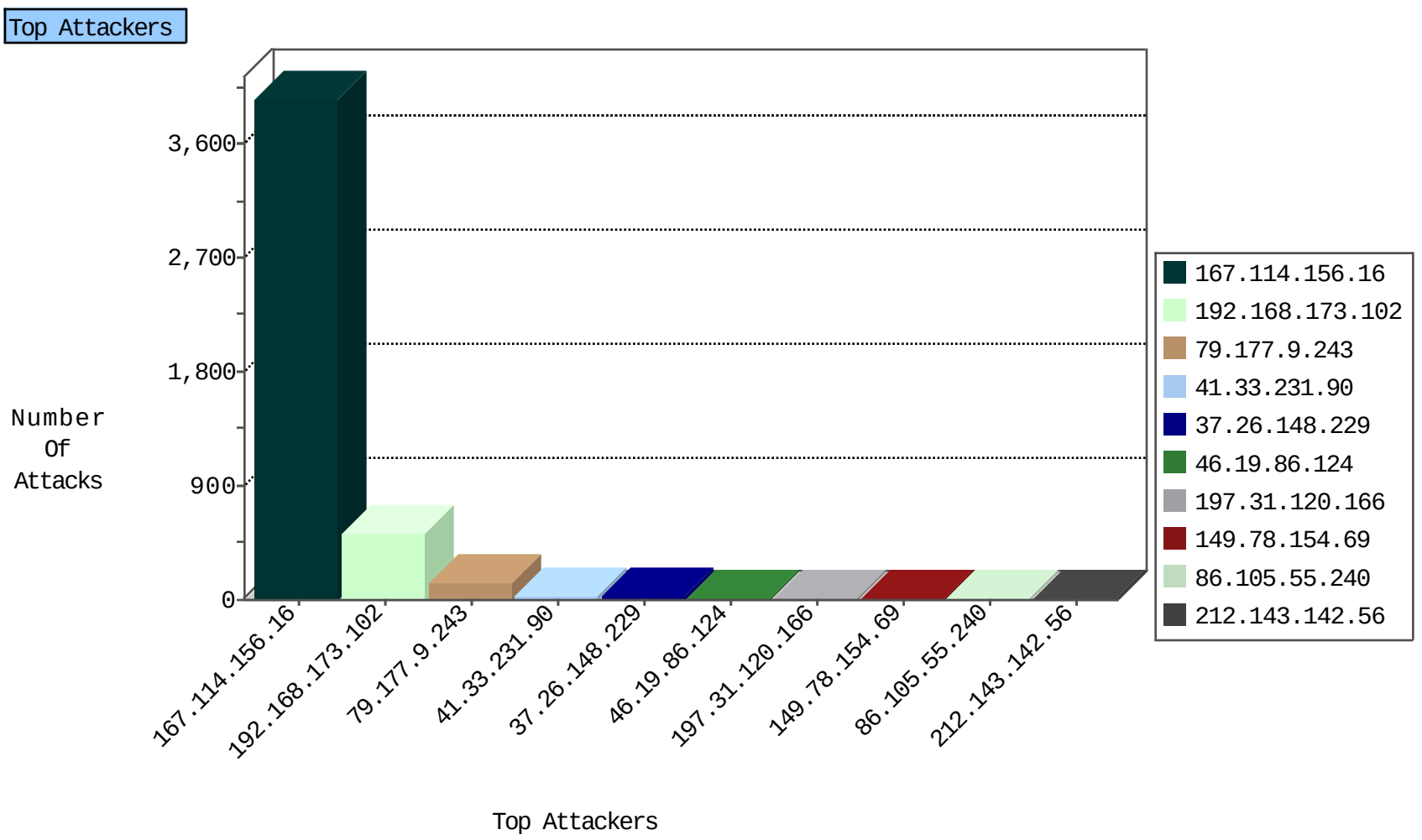
04-11-2016-00:04:00 to 04-11-2016-01:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-11-2016-00:04:00 to 04-11-2016-01:04:00

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	3960
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
93.201.95.115	Germany	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
209.213.2.1	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
115.159.150.148	China	147.237.0.19	madim.atal.idf.il	L4 Source or Dest Port Zero	drop	1
182.92.81.243	China	147.237.8.14	e.orchot.idf.il	L4 Source or Dest Port Zero	drop	1
93.201.95.115	Germany	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
219.232.243.28	China	147.237.76.34	yohalan.idf.il	L4 Source or Dest Port Zero	drop	1
115.159.150.148	China	147.237.0.35	akaws.idf.il	L4 Source or Dest Port Zero	drop	1
93.174.93.50	Netherlands	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1
190.103.170.66	Brazil	147.237.0.34	tikshuv.idf.il	Invalid TCP Flags	drop	1
110.76.40.33	China	147.237.76.30	himush.idf.il	Invalid TCP Flags	drop	1
219.232.243.28	China	147.237.77.61	e.cogat.idf.il	L4 Source or Dest Port Zero	drop	1
123.56.26.146	China	147.237.76.39	mobile.meitav.idf.il	Invalid TCP Flags	drop	1
93.201.95.115	Germany	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
190.103.170.66	Brazil	147.237.8.24	e.lifestyle.idf.il	Invalid TCP Flags	drop	1
110.76.40.33	China	147.237.76.39	mobile.meitav.idf.il	Invalid TCP Flags	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

04-11-2016-00:04:00 to 04-11-2016-01:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
5.22.135.218	Israel	147.237.72.166	aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
5.22.135.218	Israel	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1

04-11-2016-00:04:00 to 04-11-2016-01:04:00

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	3
66.249.66.56	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
185.114.157.12	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
163.172.140.23	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
86.105.55.240	147.237.77.121	Italy	e.navy.idf.il	ET SCAN Potential SSH Scan	1
86.105.55.240	147.237.76.201	Italy	e.atal.idf.il	ET SCAN Potential SSH Scan	1
86.105.55.240	147.237.76.196	Italy	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
222.73.18.162	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
86.105.55.240	147.237.76.147	Italy	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.76.31	United States	nakchal.idf.il	ET DROP Dshield Block Listed Source	1
86.105.55.240	147.237.8.50	Italy	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
187.245.153.141	147.237.8.14	Mexico	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.125.216.50	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.114.157.12	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
86.105.55.240	147.237.77.176	Italy	matpash.idf.il	ET SCAN Potential SSH Scan	1
86.105.55.240	147.237.77.19	Italy	law-forum.idf.il	ET SCAN Potential SSH Scan	1
86.105.55.240	147.237.76.197	Italy	e.himush.idf.il	ET SCAN Potential SSH Scan	1
86.105.55.240	147.237.76.177	Italy	ncore.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
86.105.55.240	147.237.76.39	Italy	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.125.216.50	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN NMAP -sS window 1024	1

04-11-2016-00:04:00 to 04-11-2016-01:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	338
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	176
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
46.19.86.124	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.253.207.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
197.31.120.166	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.219.117.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
37.26.149.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.219.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
132.66.235.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.93.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
197.31.120.166	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.32.179.108	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.22.130.79	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.13.0	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
87.69.54.96	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.22.130.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.142.33	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.81.21.217	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.28.158.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.244.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.18.207	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.26.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.151.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.254.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
109.65.106.134	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
62.219.132.191	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.22.130.79	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
5.41.128.34	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
5.22.130.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.116.141.80	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
37.26.147.221	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
217.69.133.245	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
94.230.86.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.90	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
82.81.21.217	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.139	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.253.194.33	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
106.186.113.132	Japan	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.3.144.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
85.130.221.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.199	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
73.188.210.64	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
222.73.18.162	China	147.237.0.33	idf.il	drop		drop	1

04-11-2016-00:04:00 to 04-11-2016-01:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.9.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	136
37.26.148.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
2.52.129.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
109.253.202.92	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	5
37.26.148.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.138.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-14149-he/dover.aspx	Block	1
79.181.21.78	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/926-he/refuah.aspx	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
89.139.158.184	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files	Block	1
141.212.122.129	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to /x	Block	1
66.249.78.137	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/home/default.aspx	Block	1
89.247.123.175	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/an..	Block	1
54.153.33.145	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
198.58.102.156	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
2.54.131.58	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	1
104.236.220.125	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/894-he/nakhal.aspxshared/usercontrols/headerupper/	Block	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
207.46.13.106	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1

04-11-2016-00:04:00 to 04-11-2016-01:04:00