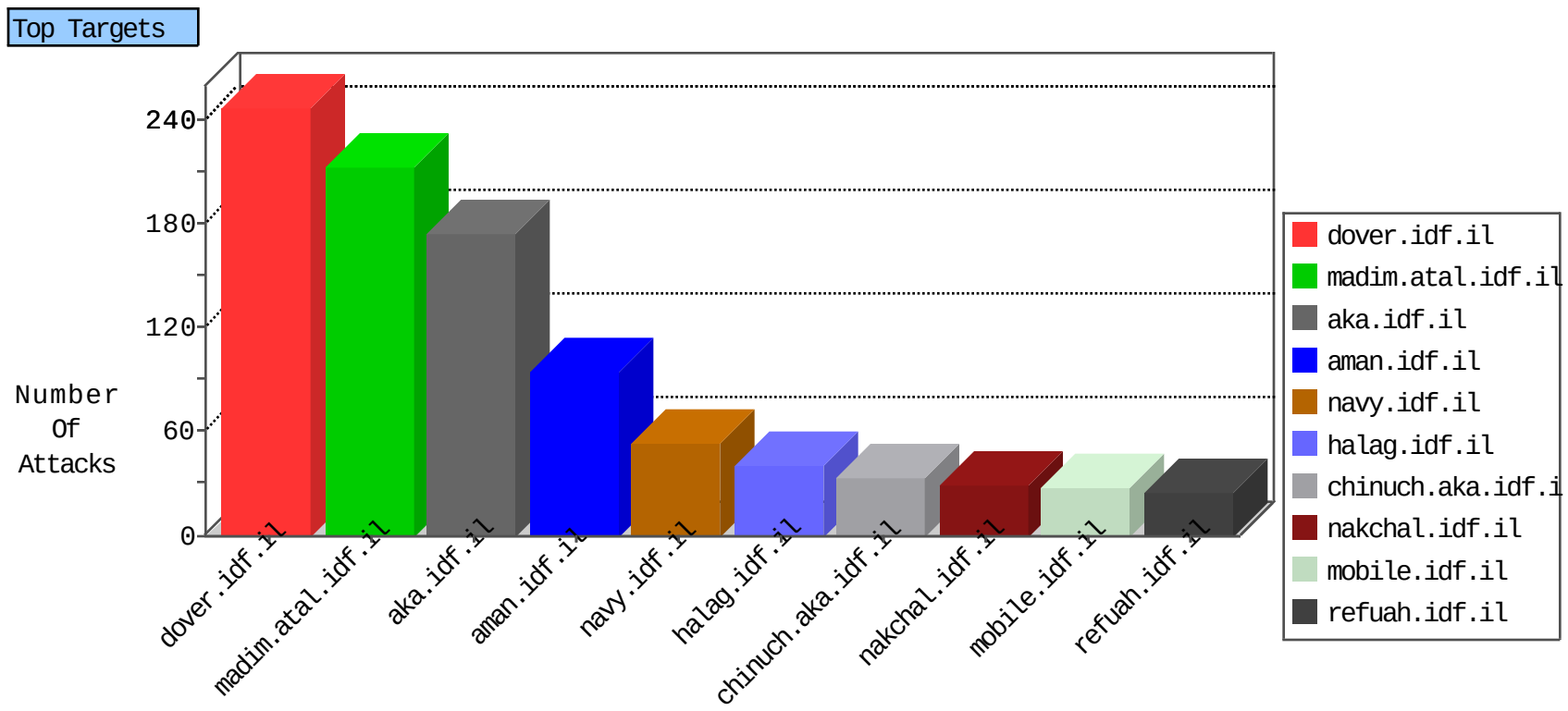
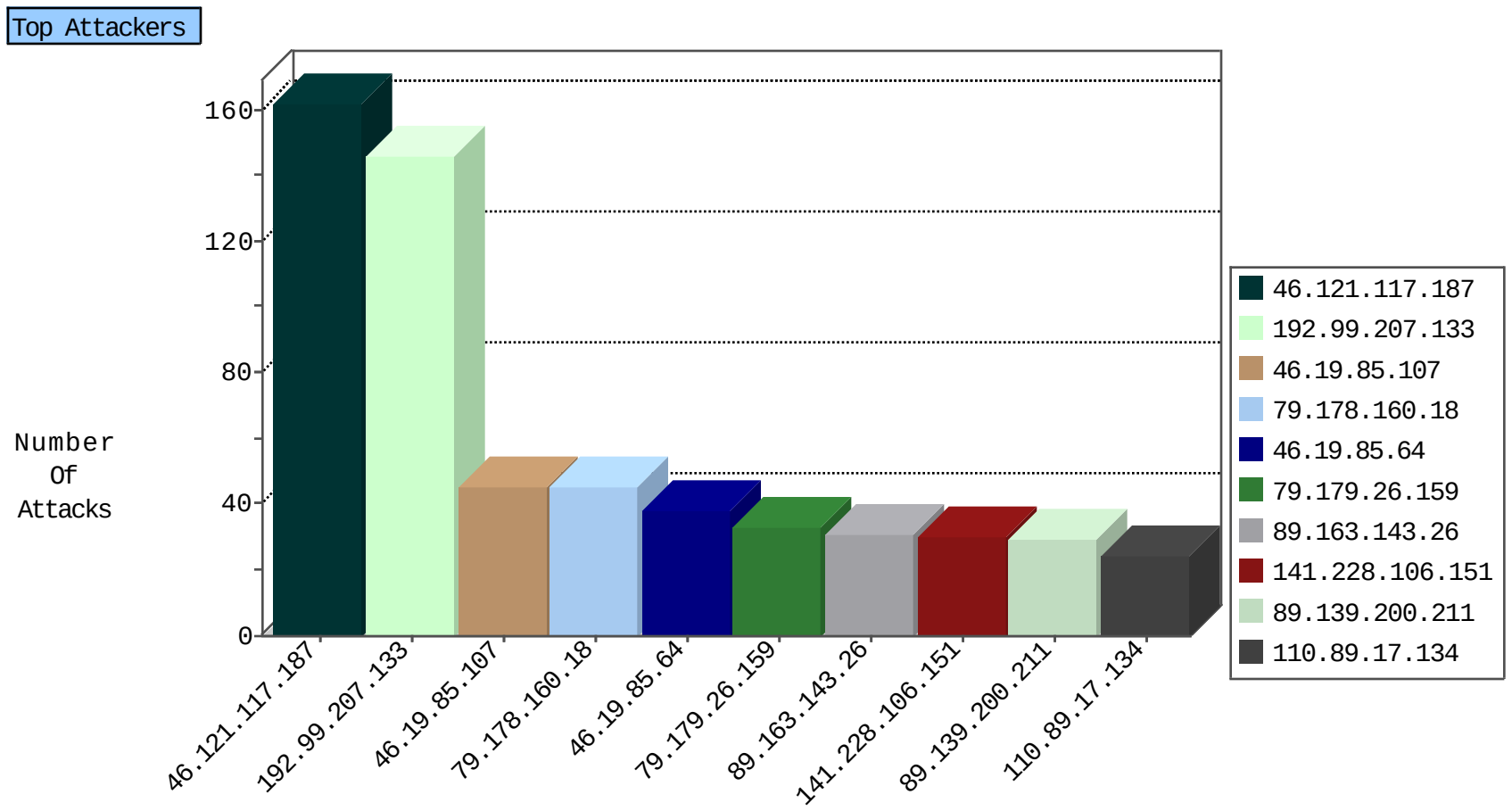
09-06-2016-19:04:08 to 09-06-2016-20:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-06-2016-19:04:08 to 09-06-2016-20:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
159.104.163.19	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.94.111.1	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
159.104.163.20	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.128.40.162	Switzerland	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
159.104.163.17	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.104.163.21	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.104.163.18	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.104.163.22	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

09-06-2016-19:04:08 to 09-06-2016-20:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.165.197.142	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-06-2016-19:04:08 to 09-06-2016-20:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	2
120.236.19.2	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -f -sS	1
80.246.133.128	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
50.116.123.135	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
12.68.215.78	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.208.193	147.237.76.198	Russian Federation	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.208.193	147.237.8.45	Russian Federation	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
120.236.19.10	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
120.236.19.2	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
93.174.94.142	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
64.137.171.55	147.237.76.86	Canada	navy.idf.il	ET SCAN Potential SSH Scan	1
47.88.33.147	147.237.77.234	Canada	halag.idf.il	ET SCAN NMAP -sS window 4096	1
45.79.111.169	147.237.77.170	United States	maarachot.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
198.52.97.92	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
195.88.208.193	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
186.170.223.196	147.237.77.121	Colombia	e.navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
120.236.19.10	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -f -sS	1

09-06-2016-19:04:08 to 09-06-2016-20:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.228.106.151	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
79.178.160.18	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
141.0.14.159	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	20
79.178.160.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
79.178.227.81	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
192.99.207.133	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
192.99.207.133	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
192.99.207.133	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
192.99.207.133	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
192.99.207.133	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
46.19.85.64	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.99.207.133	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
192.99.207.133	Canada	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
46.19.85.107	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.99.207.133	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
79.179.26.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
46.19.85.64	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
79.179.26.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.134	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
79.180.186.225	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
31.154.81.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.85.107	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
80.246.133.128	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.107	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.107	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.180.186.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
79.179.26.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
89.139.222.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.59.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.171.47	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
89.139.206.56	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
31.210.186.230	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
79.178.114.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
80.246.133.128	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.58	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
79.178.114.89	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
84.229.29.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
176.13.237.164	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.22.16	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.248	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.86.87	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.130.179.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.64	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.248	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3

09-06-2016-19:04:08 to 09-06-2016-20:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.117.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	162
89.139.200.211	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	29
5.29.62.148	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	20
46.19.86.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
110.89.17.134	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 110.89.17.134	Block	17
110.247.74.71	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 110.247.74.71	Block	15
46.19.85.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
213.57.42.201	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	6
110.89.17.134	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
110.247.74.71	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	6
77.138.52.29	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	4
2.53.59.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.53.185.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.178.227.81	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
84.108.187.46	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.3.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.183.62.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
80.246.138.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.147.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
66.249.64.224	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/0/880.pdf	Block	1
178.140.152.33	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
46.19.85.141	Israel	147.237.76.31	nakchal.idf.il	Abnormally Long Request method	Block	1
95.24.31.19	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
79.180.137.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
46.19.86.149	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/mobile/templates/basket/basket.aspx	Block	1
45.79.111.169	United States	147.237.77.170	maarachot.idf.il	Malformed HTTP Header Line 1	Block	1
2.53.59.158	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
74.96.207.26	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
66.249.64.228	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
180.76.15.32	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
46.19.85.141	Israel	147.237.76.31	nakchal.idf.il	Distributed Malformed URL	Block	1
79.182.117.113	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
5.29.101.83	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
213.57.59.50	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/tmuna/	Block	1
110.247.74.71	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.asp	Block	1
45.79.111.169	United States	147.237.77.170	maarachot.idf.il	Malformed URL	Block	1
85.65.114.103	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
2.53.166.209	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jeninkilled/stn	Block	1
192.169.7.223	United States	147.237.77.176	matpash.idf.il	Unauthorized Method HEAD for 147.237.77.176/	Block	1
46.19.85.141	Israel	147.237.76.31	nakchal.idf.il	Distributed Unknown HTTP Request Method	Block	1
79.182.117.113	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.182.117.113	Block	1
27.55.19.41	Thailand	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
2.53.13.170	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1

09-06-2016-19:04:08 to 09-06-2016-20:04:08