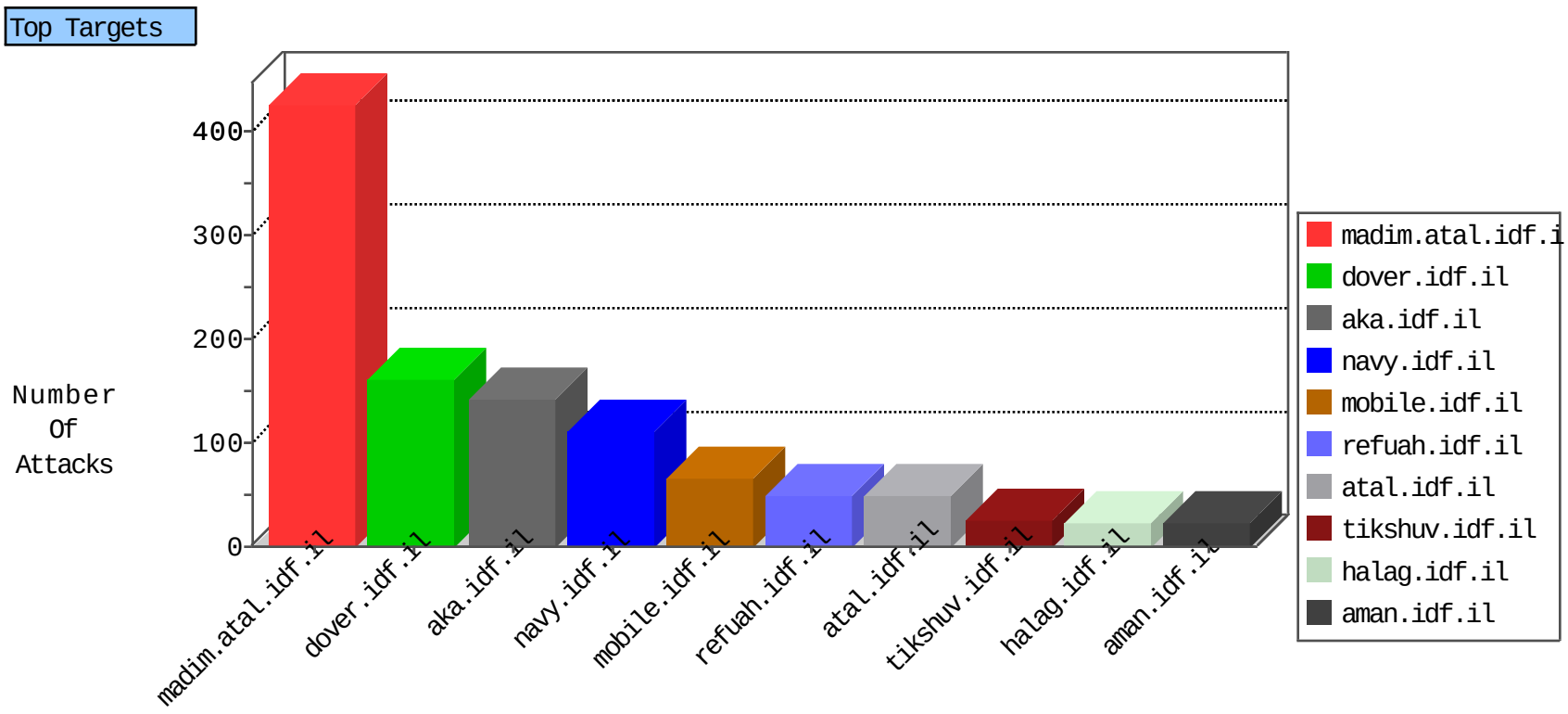
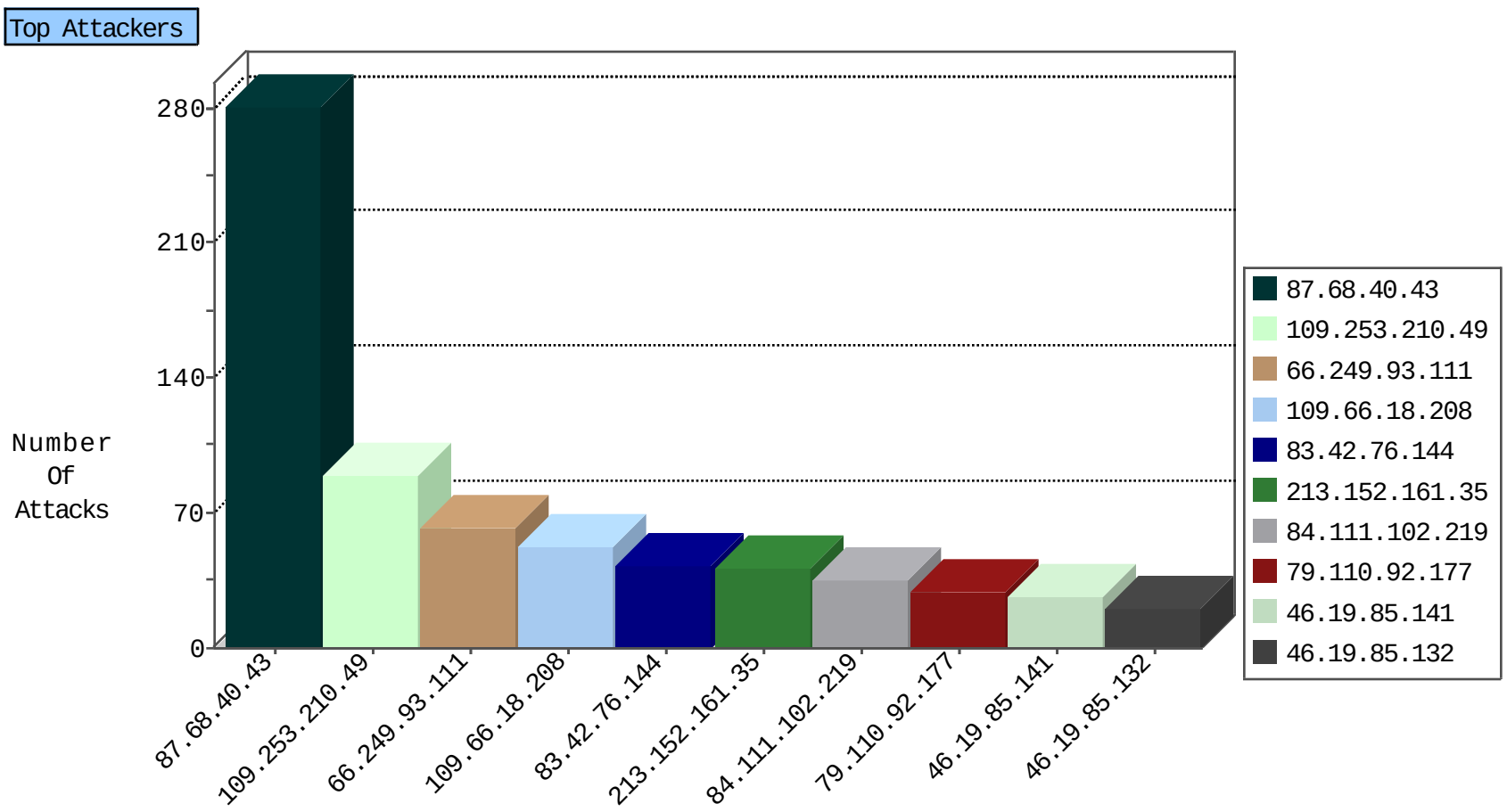
09-04-2016-20:04:01 to 09-04-2016-21:04:01

IDF Under Attack Daily Report





09-04-2016-20:04:01 to 09-04-2016-21:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.59.59.52	China	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
66.108.67.84	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
134.147.203.115	Germany	147.237.76.202	e.halag.idf.il	Black List	drop	2
114.79.9.139	Indonesia	147.237.76.39	mobile.meitav.idf.il	Black List	drop	2
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
79.176.6.113	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-04-2016-20:04:01 to 09-04-2016-21:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.129	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-04-2016-20:04:01 to 09-04-2016-21:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
151.80.41.176	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	8
91.121.144.42	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
208.100.26.228	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.135	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
162.243.85.34	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	1
109.253.129.37	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
109.60.153.178	147.237.76.39	Russian Federation	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
94.156.128.25	147.237.72.217	Bulgaria	e.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.121	Ukraine	e.navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
72.252.24.133	147.237.77.212	Jamaica	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
219.87.191.219	147.237.76.39	Taiwan	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
72.252.24.133	147.237.77.212	Jamaica	e.dover.idf.il	ET SCAN NMAP -f -sS	1
212.116.72.226	147.237.0.200	Sweden	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
50.116.123.135	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
203.86.3.66	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
46.227.67.172	147.237.72.14	Sweden	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
8.37.237.174	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.29.89	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
94.156.128.25	147.237.77.179	Bulgaria	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
219.87.191.219	147.237.76.177	Taiwan	ncore.idf.il	ET SCAN Potential SSH Scan	1
72.252.24.133	147.237.77.212	Jamaica	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
212.116.72.226	147.237.0.200	Sweden	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
50.116.123.135	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1

09-04-2016-20:04:01 to 09-04-2016-21:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.66.18.208	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	51
83.42.76.144	Spain	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	43
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	37
46.19.85.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
77.139.19.254	France	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
5.22.134.166	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
213.152.161.35	Netherlands	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	14
46.19.86.254	Israel	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
141.0.13.176	Norway	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.132	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.87	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
213.152.161.35	Netherlands	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
213.152.161.35	Netherlands	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
46.19.85.132	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.43.118.233	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.198.81	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.123	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
37.26.149.135	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.173	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.0.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.139.143.124	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.173	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
84.110.177.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.132	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
66.249.93.111	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
84.110.177.160	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.205	Israel	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	5
84.110.177.20	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
185.3.147.80	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.22.134.166	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.63	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.87	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
66.108.67.84	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
149.56.0.24	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
79.179.108.87	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
84.110.177.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.152.161.35	Netherlands	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
213.152.161.35	Netherlands	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
46.43.118.233	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
84.109.232.94	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.127	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3

09-04-2016-20:04:01 to 09-04-2016-21:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.68.40.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	281
109.253.210.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	89
84.111.102.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	32
46.19.85.28	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.85.28	Block	8
46.19.85.28	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	5
46.19.85.141	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
190.102.56.99	Panama	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	4
77.127.7.184	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/guyus	Block	3
213.57.176.125	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 213.57.176.125	Block	3
2.53.58.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.117.7.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
77.139.19.254	France	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
192.243.55.134	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	2
100.11.192.21	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
46.19.86.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.176.109.239	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mazi.idf.il	Block	1
207.46.13.45	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
46.19.85.28	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59390	Block	1
66.102.6.27	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
46.19.86.141	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
93.173.174.255	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
5.22.134.166	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.177.146.219	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19480-he/idfgdover.aspx	Block	1
213.57.176.125	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
157.55.39.167	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/english/pages/default.aspx	Block	1
46.120.61.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.64.251.174	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.87.52	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.102.9.30	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
46.19.86.141	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version 04 Sep 2016 17:16:24 GMT	Block	1
79.180.212.14	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
176.13.0.205	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	1
85.65.107.228	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/901-8008-he	Block	1
79.176.25.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage	Block	1
66.249.65.49	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter PageNum in eitan.aka.idf.il/938-en/eitan.aspx	None	1
192.243.55.135	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/default.aspx?pop=sadir	Block	1
46.19.86.141	Israel	147.237.77.216	dover.idf.il	Malformed URL sun,	Block	1
109.64.82.24	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
84.108.65.111	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
37.26.149.135	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.127.66.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.121.119.75	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catld in www.aka.idf.il/main/giyus/general.aspx	None	1
79.176.100.133	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.76.47	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/cgi-bin/shitur/bookpage100598/iturfindpageexact.pl	Block	1
199.30.25.148	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

09-04-2016-20:04:01 to 09-04-2016-21:04:01