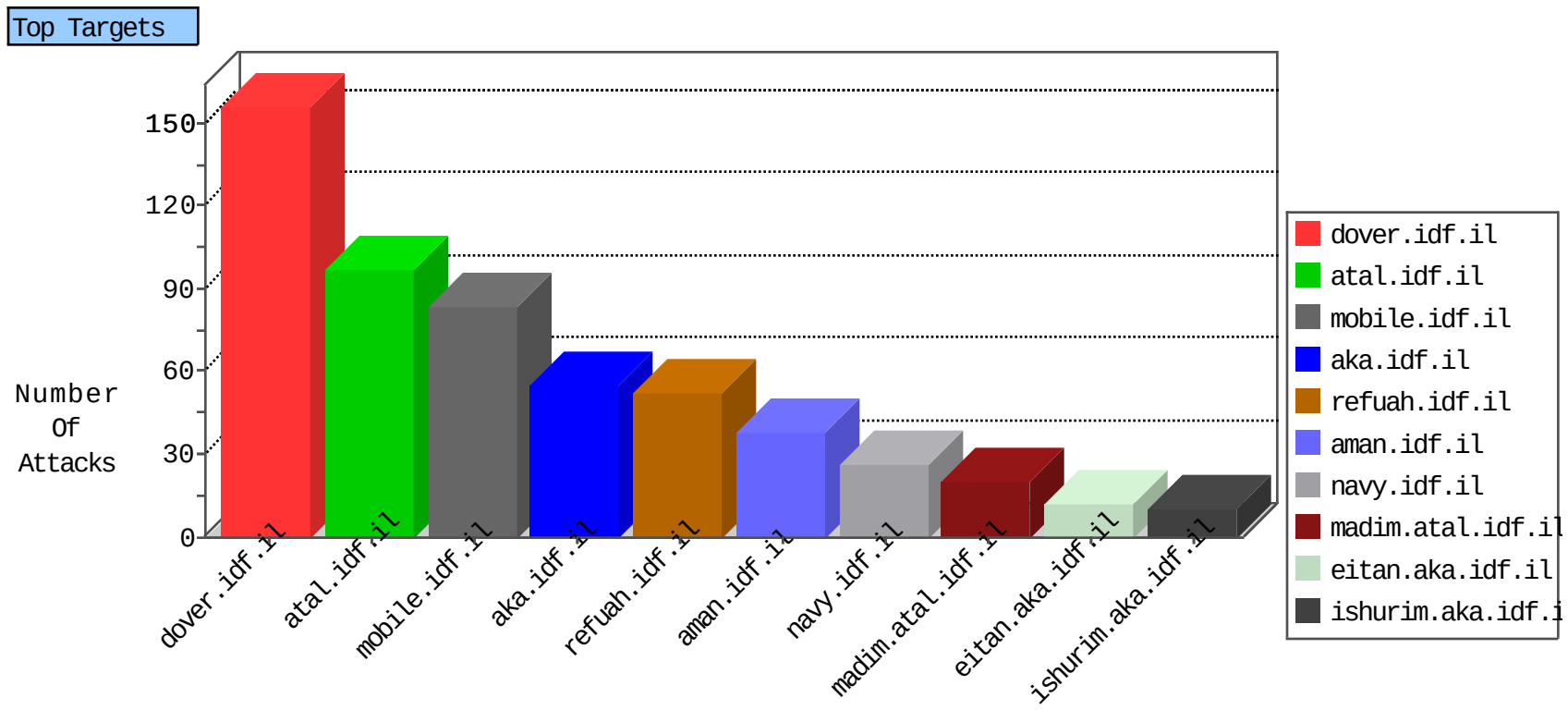
09-23-2016-10:04:00 to 09-23-2016-11:04:00

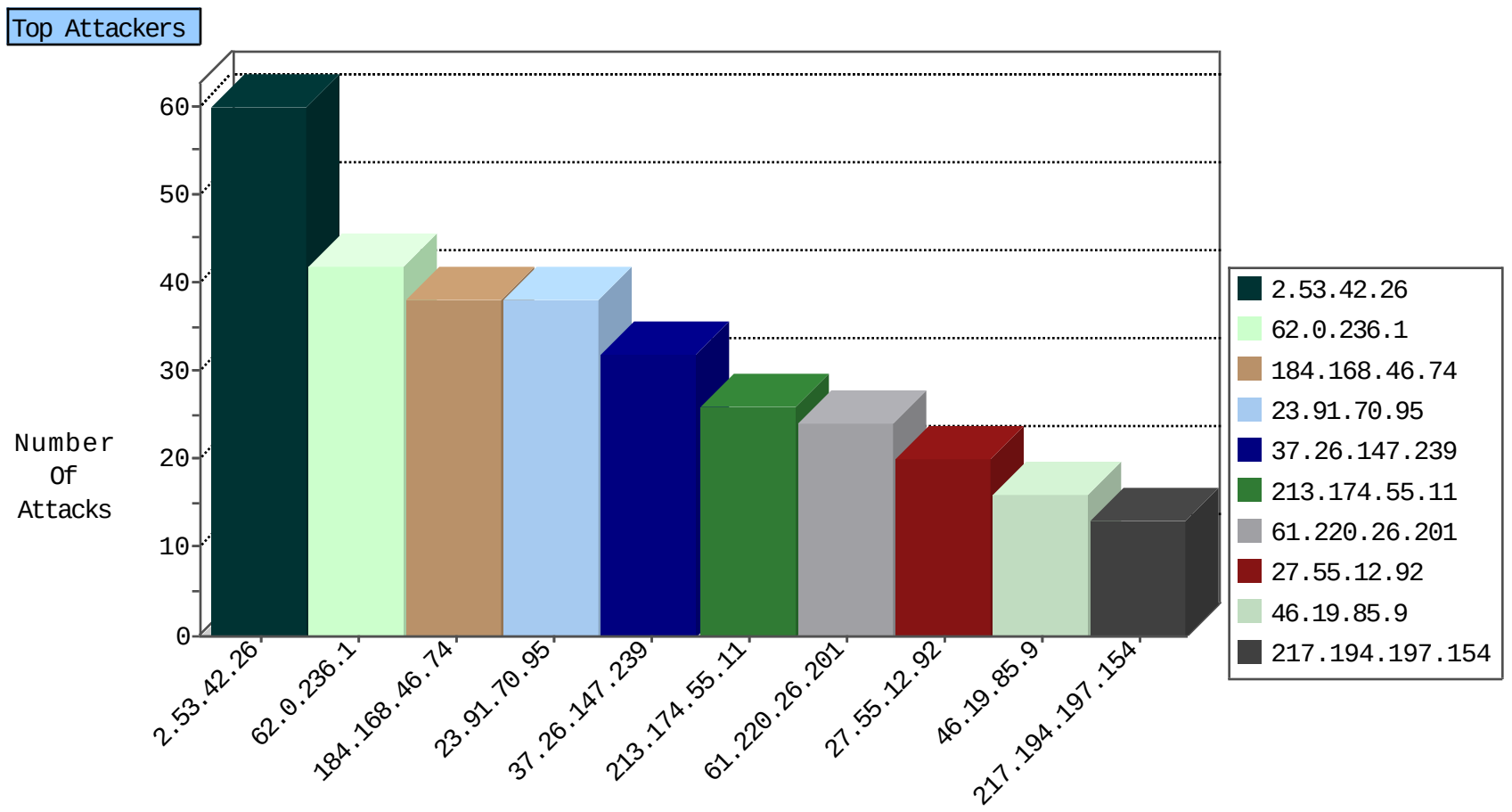
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-23-2016-10:04:00 to 09-23-2016-11:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.244.198.5	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1

09-23-2016-10:04:00 to 09-23-2016-11:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.91.70.95	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
213.174.55.11	Germany	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
61.220.26.201	Taiwan	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	11
184.168.46.74	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
184.168.46.74	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.46.74	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
23.91.70.95	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
23.91.70.95	United States	147.237.76.42	refuah.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

09-23-2016-10:04:00 to 09-23-2016-11:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
23.91.70.95	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	20
184.168.46.74	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	20
213.174.55.11	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	14
61.220.26.201	147.237.77.233	Taiwan	atal.idf.il	SQL Injection - Select From	13
128.232.110.28	147.237.72.217	United Kingdom	e.idf.il	ET SCAN Potential SSH Scan	2
115.208.231.65	147.237.77.235	China	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
128.232.110.28	147.237.76.177	United Kingdom	ncore.idf.il	ET SCAN Potential SSH Scan	1
109.236.86.32	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
100.13.130.4	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
41.215.36.46	147.237.76.31	Kenya	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.231.57	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
139.162.187.89	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
128.232.110.28	147.237.76.147	United Kingdom	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.74.129.245	147.237.76.147	Iran, Islamic Republic of	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
41.215.36.46	147.237.76.39	Kenya	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
211.149.246.60	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1

09-23-2016-10:04:00 to 09-23-2016-11:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.42.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
62.0.236.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
27.55.12.92	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
37.26.147.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
2.53.177.136	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.0.224.1	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.15.223.223	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
217.194.197.154	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
37.26.147.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.85.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
109.253.134.76	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.120.51.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.0.236.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
66.249.75.149	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.28.140	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
85.250.251.64	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
64.233.173.137	Asia/Pacific Region	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
217.194.197.141	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
217.194.197.154	Israel	147.237.76.86	navy.idf.il	SYN Attack		monitor	4
2.53.135.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.246.140.244	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.19	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
64.233.173.139	Asia/Pacific Region	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
120.188.67.202	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.42.56	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
182.55.171.59	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.147.239	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
193.106.54.33	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.117.124.208	Israel	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
80.178.101.40	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
31.168.1.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.121.253.80	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
77.237.146.28	Czech Republic	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
193.106.54.33	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
80.178.101.40	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.121.253.80	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
172.247.84.220	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
193.106.54.33	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
46.120.51.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.67.122.185	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
193.106.54.33	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.120.51.194	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
80.178.203.78	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
193.106.54.33	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.43.69.162	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
82.166.198.113	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

09-23-2016-10:04:00 to 09-23-2016-11:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.157.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
176.13.9.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
213.57.226.66	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
176.13.21.7	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	4
84.109.233.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.106	Block	3
157.55.39.155	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
77.125.26.240	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
66.249.93.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.93.83	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/assetlinks.json	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.93.83	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
204.79.180.166	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
5.29.181.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
79.177.51.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
157.55.39.26	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/sachar/klali.aspx	None	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
66.249.93.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/login.php	Block	1
213.57.214.95	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
85.65.233.40	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.233.40	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.102.9.3	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
85.65.233.40	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1148-he/chinuch.aspx	Block	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3394.jpg	Block	1
87.70.28.140	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
77.127.9.127	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb15152783 in www.aka.idf.il/main/sachar/payslips.aspx	None	1

09-23-2016-10:04:00 to 09-23-2016-11:04:00