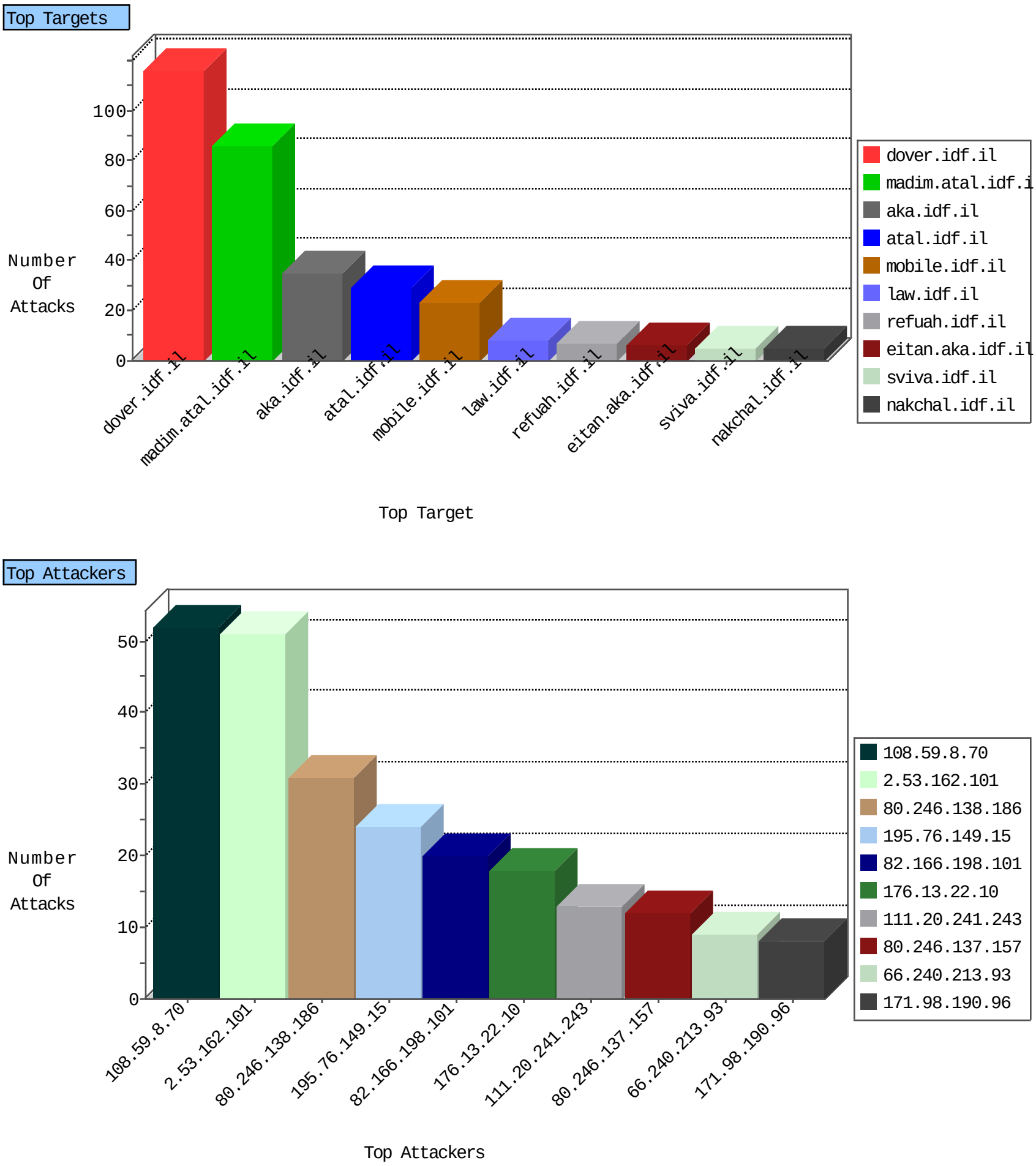
09-23-2016-01:08:58 to 09-23-2016-02:08:58

IDF Under Attack
Daily Report



09-23-2016-01:08:58 to 09-23-2016-02:08:58

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-23-2016-01:08:58 to 09-23-2016-02:08:58

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	44
195.76.149.15	Spain	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
108.59.8.70	United States	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	5
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
108.59.8.70	United States	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	3

09-23-2016-01:08:58 to 09-23-2016-02:08:58

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.76.149.15	147.237.77.233	Spain	atal.idf.il	SQL Injection - Select From	18
164.52.227.101	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
112.246.72.39	147.237.77.235	China	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.50	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
200.241.137.40	147.237.77.61	Brazil	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.73.163	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
40.121.139.43	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.239.33	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
180.97.239.33	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
164.52.227.101	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
164.52.227.101	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
104.171.124.68	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 4096	1
201.197.105.222	147.237.0.15	Costa Rica	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.50	147.237.76.200	Ukraine	eitan.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.199.89.155	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
60.185.87.142	147.237.77.235	China	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.93.185.10	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
40.121.139.43	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.239.33	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
180.97.239.33	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1

09-23-2016-01:08:58 to 09-23-2016-02:08:58

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
82.166.198.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
176.13.22.10	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
80.246.137.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
171.98.190.96	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
111.20.241.243	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
111.20.241.243	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
165.142.249.81	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
162.208.92.66	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
84.108.157.104	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
77.138.6.232	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
89.138.183.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.66.205.160	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
90.200.108.216	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.165.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
66.240.213.93	United States	147.237.77.216	dover.idf.il	Scanner Enforcement Violation	Masscan Port Scanner	reject	1
141.212.122.83	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.76.15.143	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.10	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.54	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
2.53.150.244	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
101.199.112.50	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
73.167.252.113	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.131	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.240.213.93	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.58	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
198.199.89.155	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.22.134.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
176.13.242.94	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.0.33	idf.il	drop		drop	1
66.240.213.93	United States	147.237.77.226	www.chamatz.aka.idf.il	Scanner Enforcement Violation	Masscan Port Scanner	reject	1
141.212.122.89	United States	147.237.0.35	akaws.idf.il	drop		drop	1
213.8.204.57	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.10	Israel	147.237.77.74	law.idf.il	Block HTTP Non Compliant	illegal header format detected: Illeg start line in request	monitor	1
141.212.122.55	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.76.15.162	China	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
2.53.150.244	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
109.64.139.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.132	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.240.213.93	United States	147.237.77.170	maarachot.idf.il	Scanner Enforcement Violation	Masscan Port Scanner	reject	1
141.212.122.59	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
198.199.89.155	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.102.242.4	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
176.13.247.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.0.35	akaws.idf.il	drop		drop	1
66.240.213.93	United States	147.237.77.233	atal.idf.il	Scanner Enforcement Violation	Masscan Port Scanner	reject	1
141.212.122.89	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
221.181.73.62	China	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

09-23-2016-01:08:58 to 09-23-2016-02:08:58

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.162.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	51
80.246.138.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
31.154.81.27	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	2
31.154.81.27	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	2
185.32.179.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
198.20.87.98	United States	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/robots.txt	Block	1
79.180.61.19	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
31.154.81.27	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
157.55.39.25	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	1
68.180.230.186	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/228-he/faq.aspx	Block	1
31.131.247.74	Italy	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
199.212.87.2	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 199.212.87.2	Block	1
46.19.86.10	Israel	147.237.77.74	law.idf.il	Malformed URL	Block	1
176.13.242.94	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
199.212.87.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
80.246.139.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
46.19.86.10	Israel	147.237.77.74	law.idf.il	Unknown HTTP Request Method d.browser in URL	Block	1
180.76.15.153	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/shared/clientscripts/{1}	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/default.asp	Block	1
201.240.165.207	Peru	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.19.79.201	Czech Republic	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2977.jpg	Block	1
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	1
31.154.81.27	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
89.237.88.82	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2368.jpg	Block	1

09-23-2016-01:08:58 to 09-23-2016-02:08:58