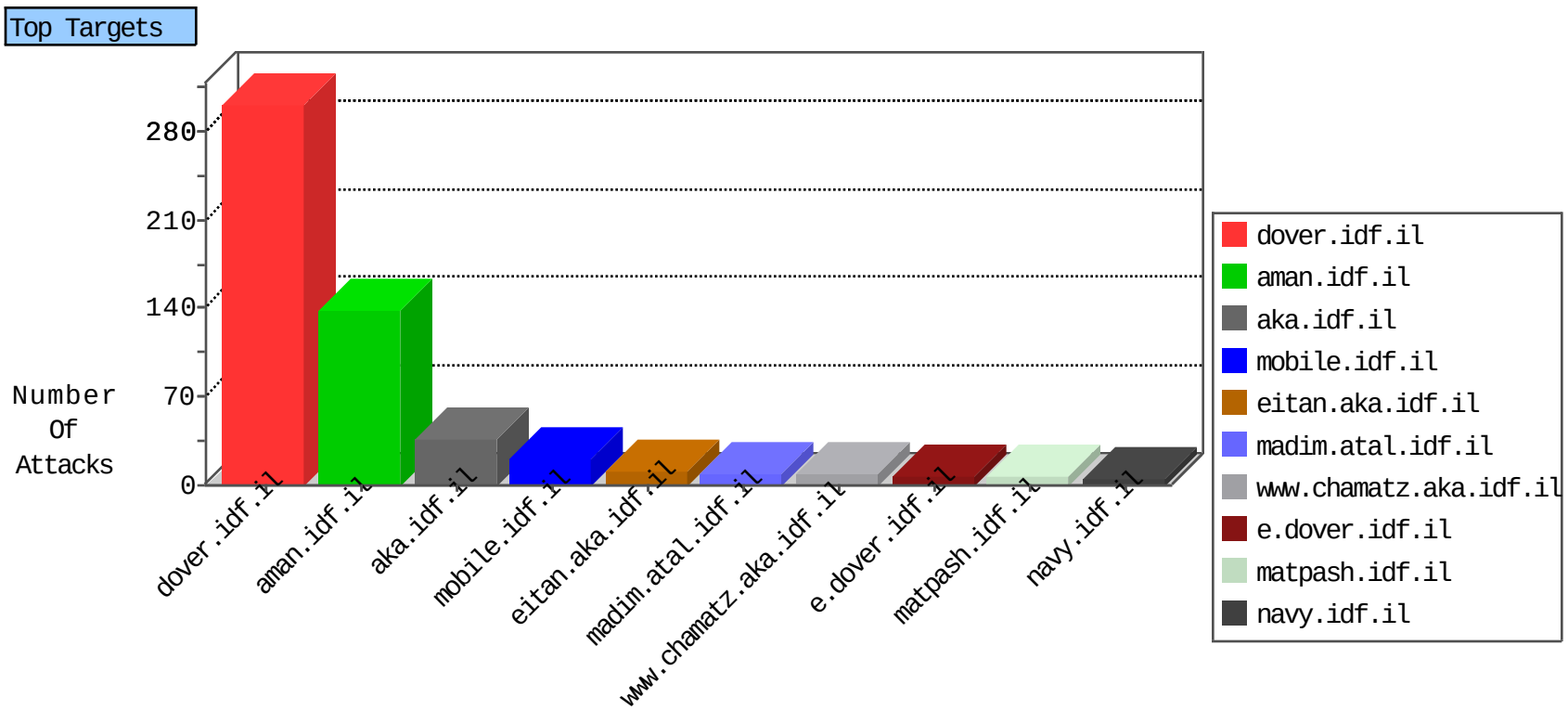
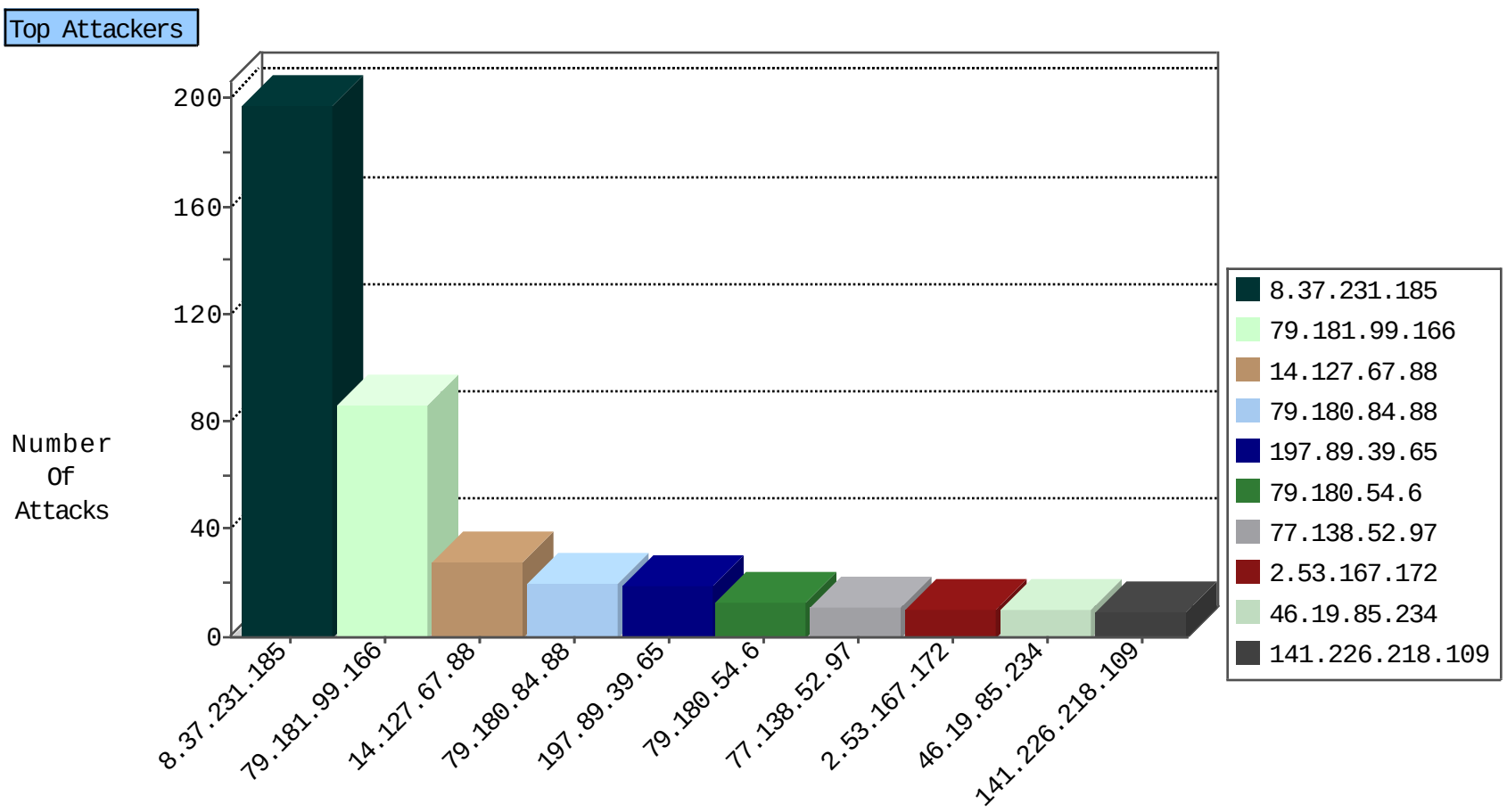
10-01-2016-10:04:01 to 10-01-2016-11:04:01

IDF Under Attack Daily Report





10-01-2016-10:04:01 to 10-01-2016-11:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
8.37.231.185	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
134.147.203.115	Germany	147.237.76.34	yohalan.idf.il	Black List	drop	2
66.240.236.119	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
37.228.91.142	Russian Federation	147.237.76.197	e.himush.idf.il	Black List	drop	1
157.55.39.201	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

10-01-2016-10:04:01 to 10-01-2016-11:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.54	Israel	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

10-01-2016-10:04:01 to 10-01-2016-11:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
95.47.140.55	147.237.76.198	Russian Federation	e.yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.110.132.201	147.237.77.216	Ukraine	dover.idf.il	ET SCAN Potential SSH Scan	1
49.73.240.131	147.237.76.86	China	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.110.132.201	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN Potential SSH Scan	1
27.2.214.44	147.237.77.226	Vietnam	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
185.110.132.201	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
8.37.231.185	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.0.33	Ukraine	idf.il	ET SCAN Potential SSH Scan	1
125.65.94.41	147.237.77.243	China	mobile.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.183.156.102	147.237.0.200	Vietnam	m4u.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.23.48.64	147.237.76.86	Vietnam	navy.idf.il	ET SCAN NMAP -f -sS	1
101.24.189.34	147.237.77.121	China	e.navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.110.132.201	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN Potential SSH Scan	1
62.210.189.248	147.237.76.202	France	e.halag.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN Potential SSH Scan	1
40.84.189.118	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.110.132.201	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
23.91.75.231	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
185.110.132.201	147.237.8.27	Ukraine	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
180.213.5.205	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
121.228.154.88	147.237.0.19	China	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.23.48.64	147.237.76.86	Vietnam	navy.idf.il	ET SCAN NMAP -sS window 2048	1
104.207.141.110	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
209.95.50.84	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

10-01-2016-10:04:01 to 10-01-2016-11:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.231.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	117
8.37.231.185	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	77
79.181.99.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
79.181.99.166	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	17
79.180.84.88	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	12
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
197.89.39.65	South Africa	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
2.53.167.172	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.180.54.6	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
141.226.218.109	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
209.133.111.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.53.183.2	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
109.253.213.90	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.63.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
185.3.147.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.29.216.253	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.137	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
193.43.246.250	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
197.89.39.65	South Africa	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
31.13.113.128	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.116.48.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
185.3.147.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.234	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
187.61.127.162	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.116.48.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.63.237.203	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
197.89.39.65	South Africa	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.138.52.97	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.218.248	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.9	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
187.61.127.154	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
122.162.245.63	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
88.212.37.65	Slovakia	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
187.61.127.157	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
77.138.236.8	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
197.89.39.65	South Africa	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
93.158.200.68	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
14.127.67.88	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
157.55.39.201	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

10-01-2016-10:04:01 to 10-01-2016-11:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
14.127.67.88	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 14.127.67.88	Block	19
14.127.67.88	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	7
79.180.54.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.108.117.91	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.108.117.91	Block	2
109.253.213.90	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.66.49.63	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.180.84.88	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Method 6¢øW9§]i	Block	1
66.249.65.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8847-he/refuah.aspx	Block	1
213.8.204.30	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
79.180.84.88	Israel	147.237.72.156	aman.idf.il	Distributed Malformed HTTP Header Line	Block	1
46.19.86.35	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
79.180.84.88	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.108.117.91	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/gius	Block	1
79.180.84.88	Israel	147.237.72.156	aman.idf.il	Distributed Malformed URL	Block	1
46.121.198.138	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.164	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
79.180.84.88	Israel	147.237.72.156	aman.idf.il	Too Many Headers per Request - 62 Headers	Block	1
109.64.56.239	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
79.180.84.88	Israel	147.237.72.156	aman.idf.il	Distributed Unknown HTTP Request Method	Block	1
52.78.164.22	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/web-console/serverinfo.jsp	Block	1
185.120.125.63	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 79.181.99.166 (Open Mode)	None	1
79.180.54.6	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
40.77.167.64	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
109.65.21.253	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	1
79.180.84.88	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Value	Block	1
66.249.65.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
213.8.204.30	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
79.181.99.166	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.180.84.88	Israel	147.237.72.156	aman.idf.il	Abnormally Long Header Line request header name	Block	1

10-01-2016-10:04:01 to 10-01-2016-11:04:01