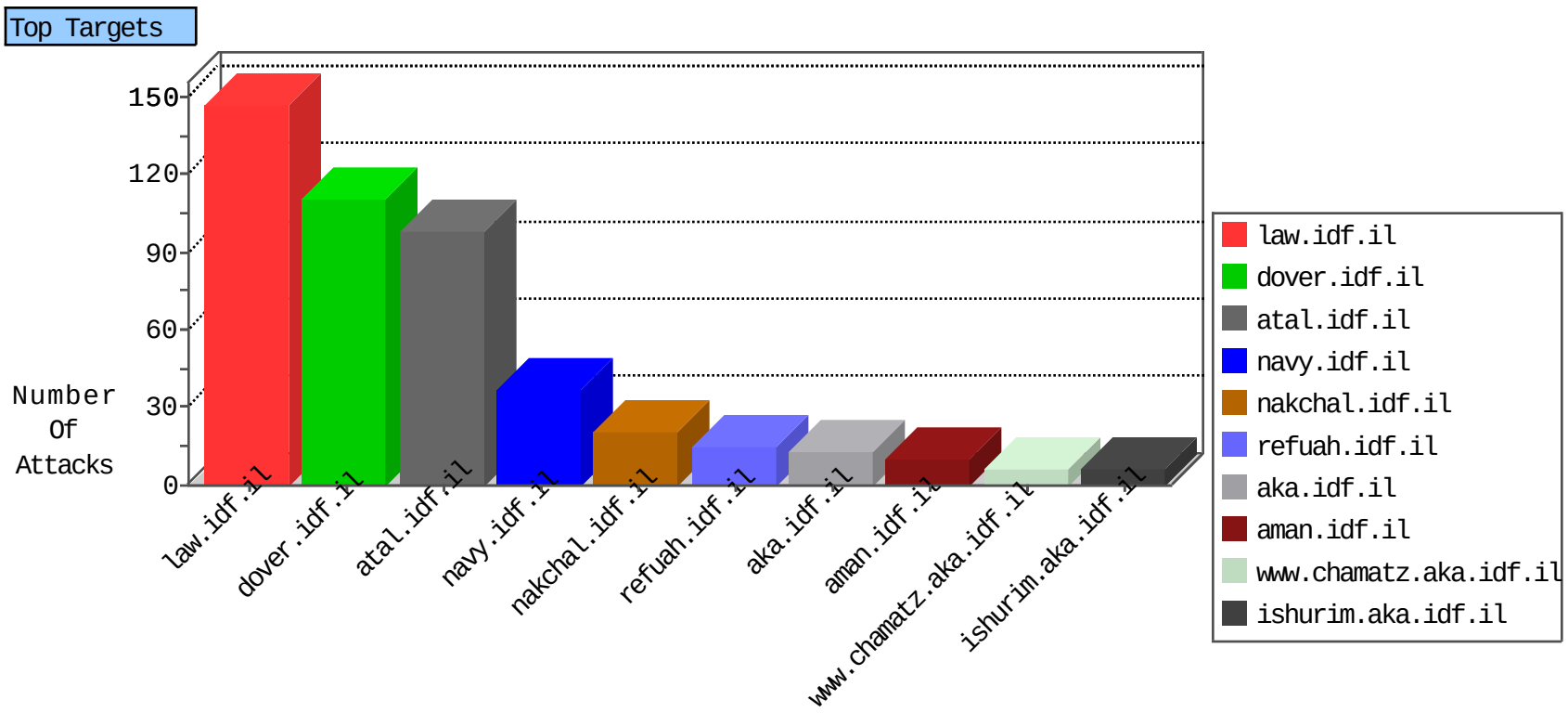
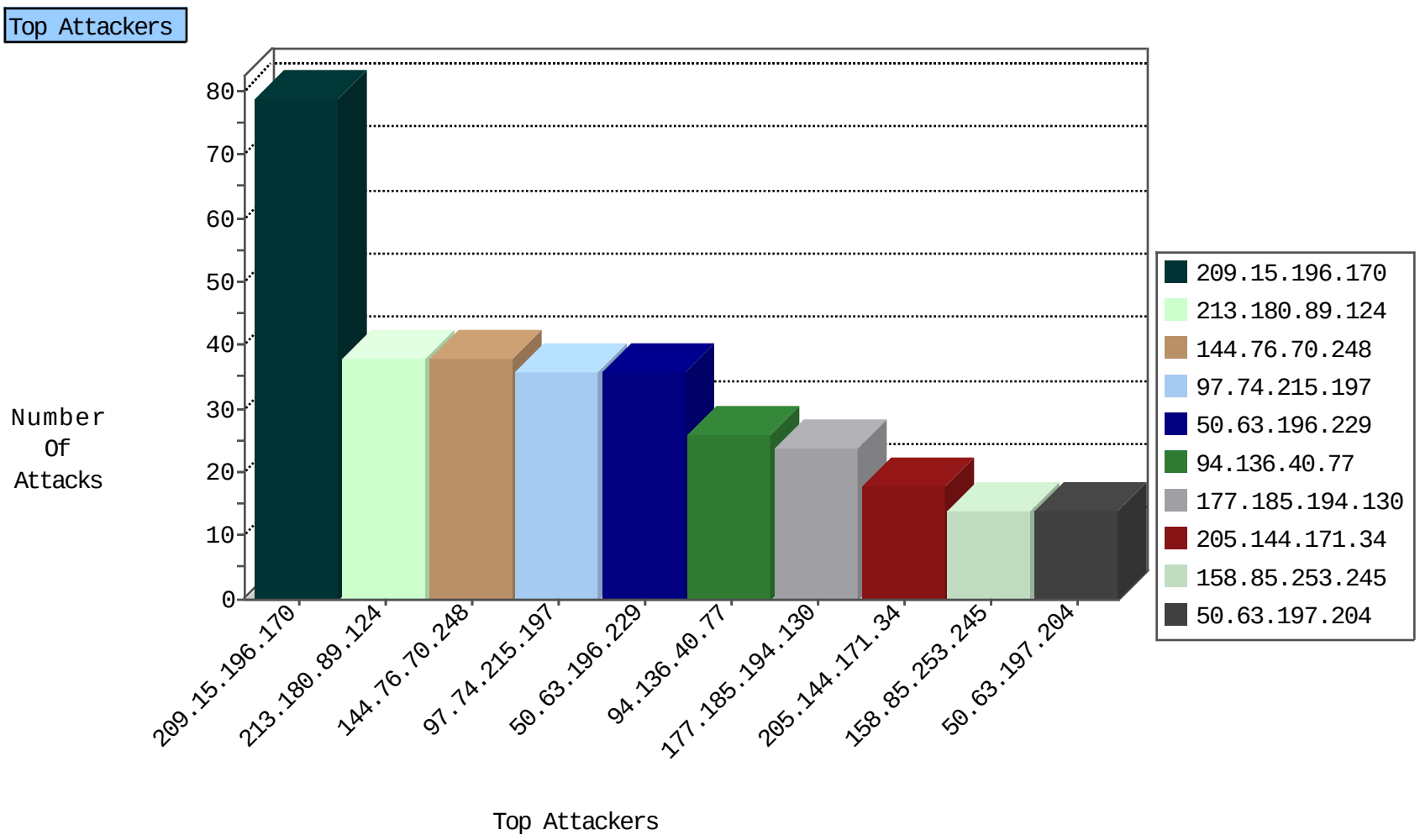
09-23-2016-02:04:02 to 09-23-2016-03:04:02

IDF Under Attack
Daily Report





09-23-2016-02:04:02 to 09-23-2016-03:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
183.60.48.25	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
58.221.61.155	China	147.237.77.178	e.matpash.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

09-23-2016-02:04:02 to 09-23-2016-03:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.180.89.124	Sweden	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
50.63.196.229	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
209.15.196.170	Canada	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
144.76.70.248	Germany	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
94.136.40.77	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
97.74.215.197	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
158.85.253.245	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.15.196.170	Canada	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
97.74.215.197	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.185.194.130	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.197.204	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.15.196.170	Canada	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.77	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
202.124.109.87	New Zealand	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
69.7.43.246	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
144.76.70.248	Germany	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.15.196.170	Canada	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
91.151.208.90	United Kingdom	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
213.180.89.124	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.15.196.170	Canada	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.196.229	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
5.9.8.150	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
36.110.147.83	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-23-2016-02:04:02 to 09-23-2016-03:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.15.196.170	147.237.77.233	Canada	atal.idf.il	SQL Injection - Select From	21
144.76.70.248	147.237.77.216	Germany	dover.idf.il	SQL Injection - Select From	20
213.180.89.124	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	20
209.15.196.170	147.237.77.216	Canada	dover.idf.il	SQL Injection - Select From	20
97.74.215.197	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	19
50.63.196.229	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	19
177.185.194.130	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	18
94.136.40.77	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	14
69.7.43.246	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
50.63.197.204	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
158.85.253.245	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
91.151.208.90	147.237.77.233	United Kingdom	atal.idf.il	SQL Injection - Select From	8
202.124.109.87	147.237.76.42	New Zealand	refuah.idf.il	SQL Injection - Select From	8
23.91.70.77	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
91.201.236.155	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
46.183.223.228	147.237.72.14	Latvia	dover.idf.il(old	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.72.156	Cote D'Ivoire	aman.idf.il	ET SCAN NMAP -sS window 4096	1
196.47.173.21	147.237.72.156	Cote D'Ivoire	aman.idf.il	ET SCAN NMAP -f -sS	1
128.232.110.28	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN Potential SSH Scan	1
222.191.157.90	147.237.76.177	China	ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.76.83	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
196.47.173.21	147.237.72.156	Cote D'Ivoire	aman.idf.il	ET SCAN NMAP -sS window 2048	1

09-23-2016-02:04:02 to 09-23-2016-03:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
205.144.171.34	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	18
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
84.245.33.104	Netherlands	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
42.236.10.71	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
42.236.10.71	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.56	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
37.26.146.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
162.208.92.66	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
42.236.10.98	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
42.236.10.98	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
42.236.10.100	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
2.53.8.77	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
42.236.10.100	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
2.55.5.61	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
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
46.117.0.179	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.55	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
66.240.213.93	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.76.15.27	China	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
37.46.41.132	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.85	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.137	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.56	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
66.240.213.93	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
195.60.235.58	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.89	United States	147.237.0.35	akaws.idf.il	drop		drop	1
85.64.151.114	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.138	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.57	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.179.108.202	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
198.20.69.74	United States	147.237.8.24	e.lifestyle.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.90	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.53	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
221.181.73.62	China	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	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
169.229.3.91	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.94	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.54	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.84	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
84.108.157.104	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-23-2016-02:04:02 to 09-23-2016-03:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
47.139.7.244	Canada	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
89.237.88.82	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
140.168.79.1	Australia	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
45.79.181.240	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteyerua/	Block	1
207.46.13.49	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
68.180.230.216	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
207.46.13.190	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/halochamim	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.102.9.8	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
77.138.245.99	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
182.18.151.54	India	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/3470.jpg	Block	1
182.18.151.54	India	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/changelog.txt	Block	1
66.249.75.38	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/imagevideogallerylobby/imagevideogallerylobby.aspx	Block	1

09-23-2016-02:04:02 to 09-23-2016-03:04:02