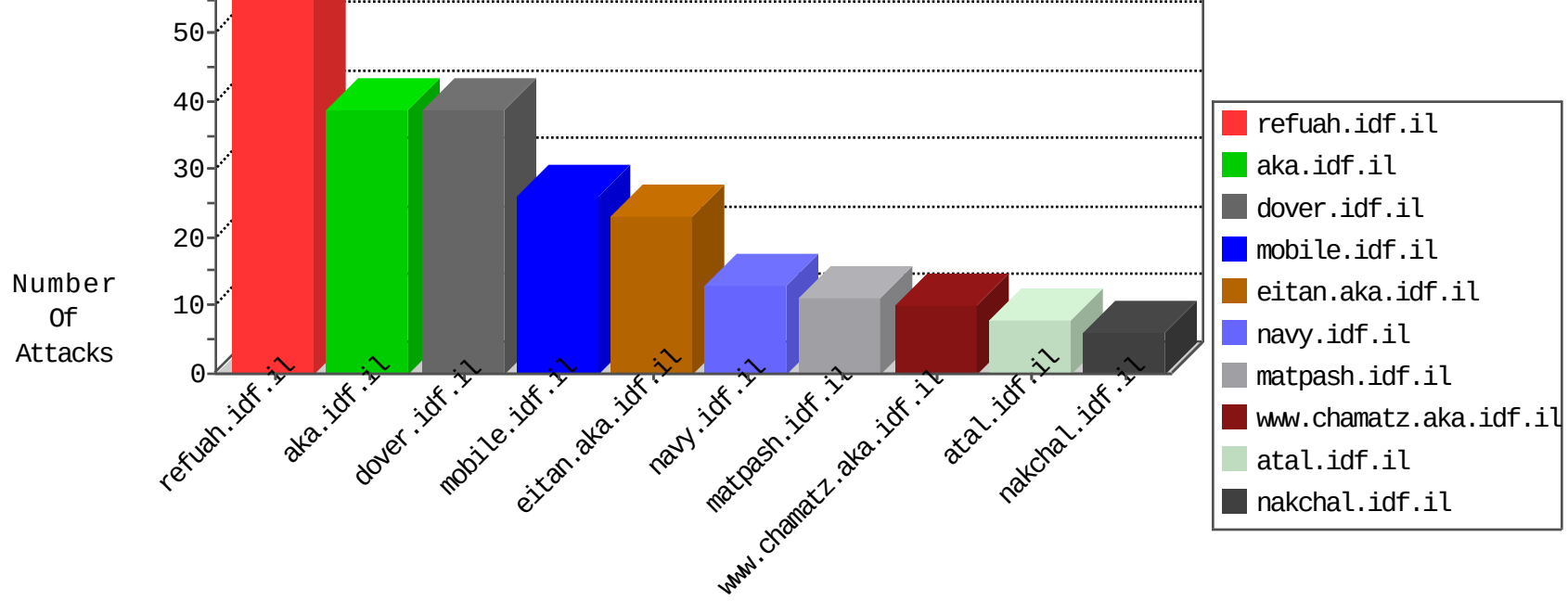
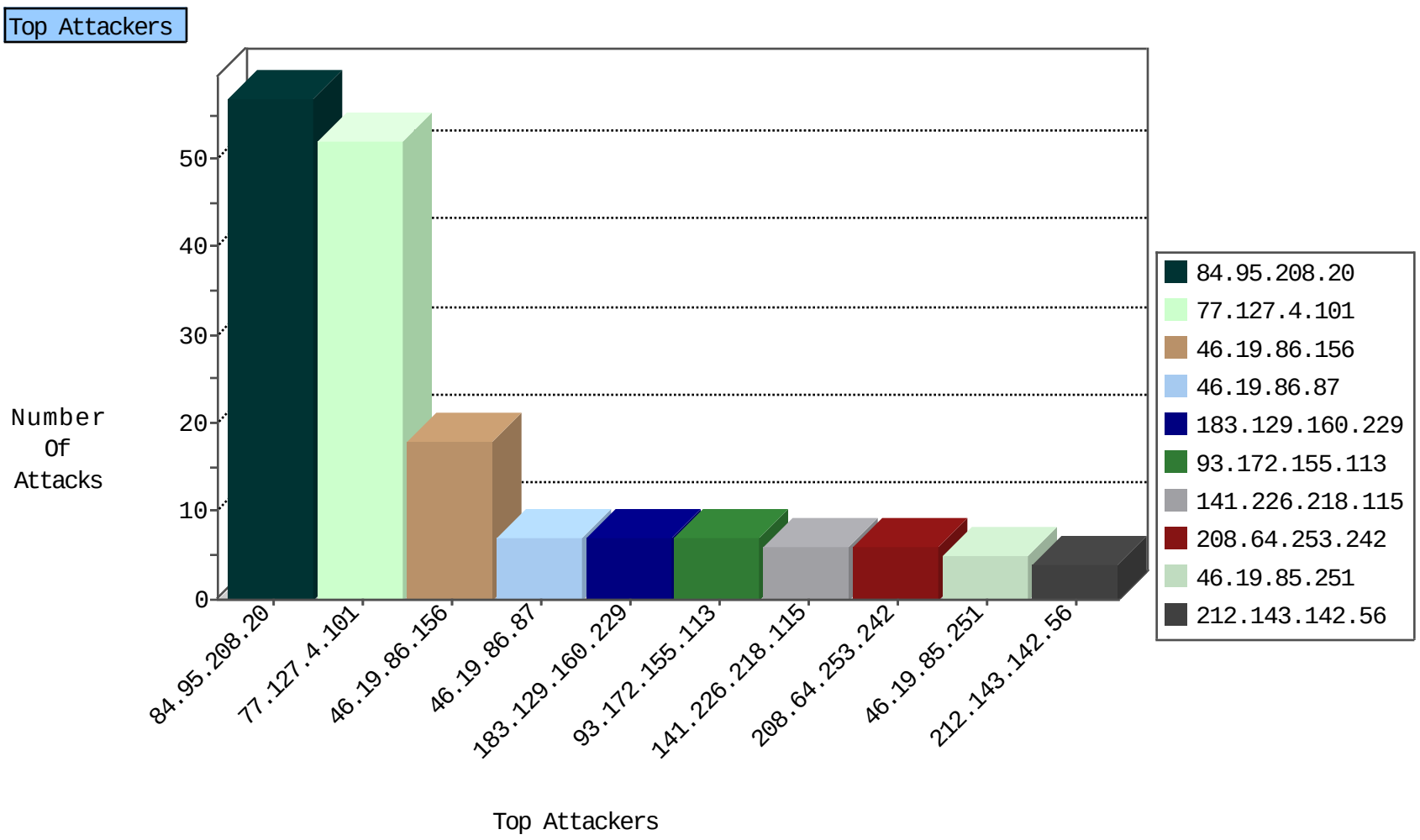
10-04-2016-09:04:04 to 10-04-2016-10:04:04

IDF Under Attack Daily Report





10-04-2016-09:04:04 to 10-04-2016-10:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.130	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	2
195.62.53.168	Russian Federation	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
113.109.113.82	China	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.42	refuah.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.177	ncore.idf.il	Black List	drop	1

10-04-2016-09:04:04 to 10-04-2016-10:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-04-2016-09:04:04 to 10-04-2016-10:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.121.143.113	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
146.200.148.0	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
208.64.253.242	147.237.76.200	United States	eitan.aka.idf.il	Admin login page scan - Havij	1
208.64.253.242	147.237.76.39	United States	mobile.meitav.idf.il	Admin login page scan - Havij	1
85.113.113.31	147.237.77.233	Palestinian Territory, Occupied	atal.idf.il	ET SCAN NMAP -sA (2)	1
208.64.253.242	147.237.76.30	United States	himush.idf.il	Admin login page scan - Havij	1
62.210.243.100	147.237.77.61	France	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
200.195.135.82	147.237.8.50	Brazil	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
45.76.2.156	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
200.195.135.82	147.237.8.50	Brazil	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
14.152.59.11	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.236.86.32	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
208.64.253.242	147.237.77.216	United States	dover.idf.il	Admin login page scan - Havij	1
91.201.236.50	147.237.76.201	Ukraine	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
208.64.253.242	147.237.76.42	United States	refuah.idf.il	Admin login page scan - Havij	1
89.248.163.3	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
208.64.253.242	147.237.76.31	United States	nakchal.idf.il	Admin login page scan - Havij	1
66.249.76.108	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
202.57.162.182	147.237.76.31	Thailand	nakchal.idf.il	ET SCAN Potential SSH Scan	1
54.82.56.247	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
200.195.135.82	147.237.8.50	Brazil	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
45.76.2.156	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
180.213.5.205	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
115.239.251.250	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
109.236.86.32	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.50	147.237.76.201	Ukraine	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1

10-04-2016-09:04:04 to 10-04-2016-10:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.127.4.101	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
46.19.86.156	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
93.172.155.113	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.251	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
77.138.8.96	France	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.110.108.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
141.226.218.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.134.222	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.245.246.13	Turkey	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
80.246.133.47	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
178.245.195.29	Turkey	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
122.179.183.154	India	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
109.67.251.7	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.87	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
188.56.199.51	Turkey	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
79.180.255.211	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.64.152.251	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
178.245.191.170	Turkey	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
199.30.25.121	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
141.212.122.42	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.64.166.72	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
183.129.160.229	China	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.109	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.46.38.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
207.46.13.46	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
89.138.71.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
183.129.160.229	China	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
176.13.229.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.87	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.102	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.22.134.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.117.126.39	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.110	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.46.38.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
122.179.183.154	India	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
93.172.155.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
183.129.160.229	China	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.180.8.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP anomaly detected	Non-compliant TCP packets coming from multiple external sources were detected. This may result from potential network configuration problem.	drop	1
178.245.174.196	Turkey	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.103	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
31.210.187.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
178.245.246.199	Turkey	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
46.117.126.39	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

10-04-2016-09:04:04 to 10-04-2016-10:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
24.20.124.102	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	3
141.226.218.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	2
87.71.41.153	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
77.127.4.101	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
109.67.18.203	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/69738.pdf	Block	1
87.69.24.253	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/forums.frm/frmprintmessage.aspx	Block	1
77.139.180.196	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
40.77.167.66	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
68.180.229.234	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/62312	Block	1
87.71.41.153	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 87.71.41.153	Block	1
157.55.39.92	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.92	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/69141.pdf	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
77.126.28.138	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/guyus	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
195.62.53.168	Russian Federation	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to gmail.com/engine/log.txt	Block	1
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/69069.pdf	Block	1
77.127.4.101	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
87.71.41.153	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	1
24.20.124.102	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 24.20.124.102	Block	1

10-04-2016-09:04:04 to 10-04-2016-10:04:04