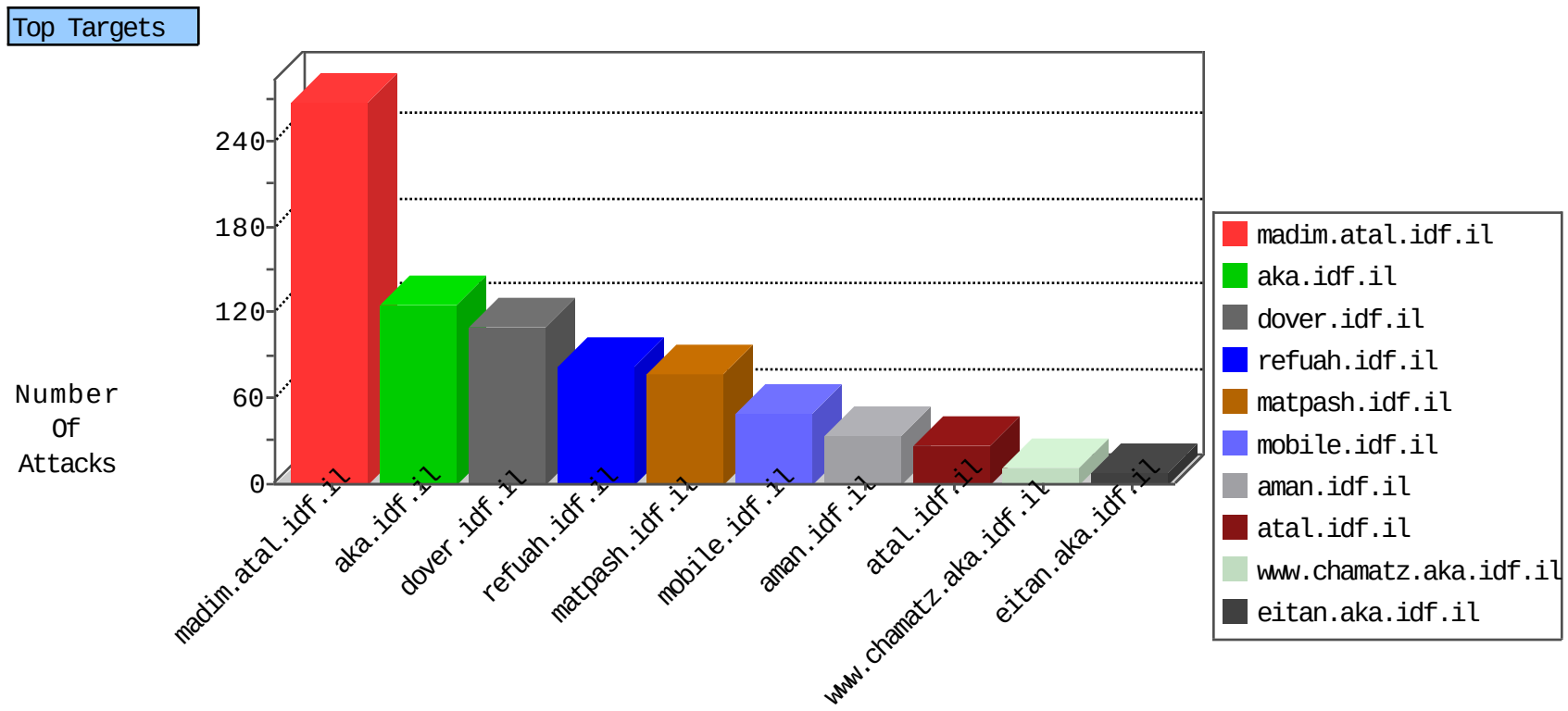
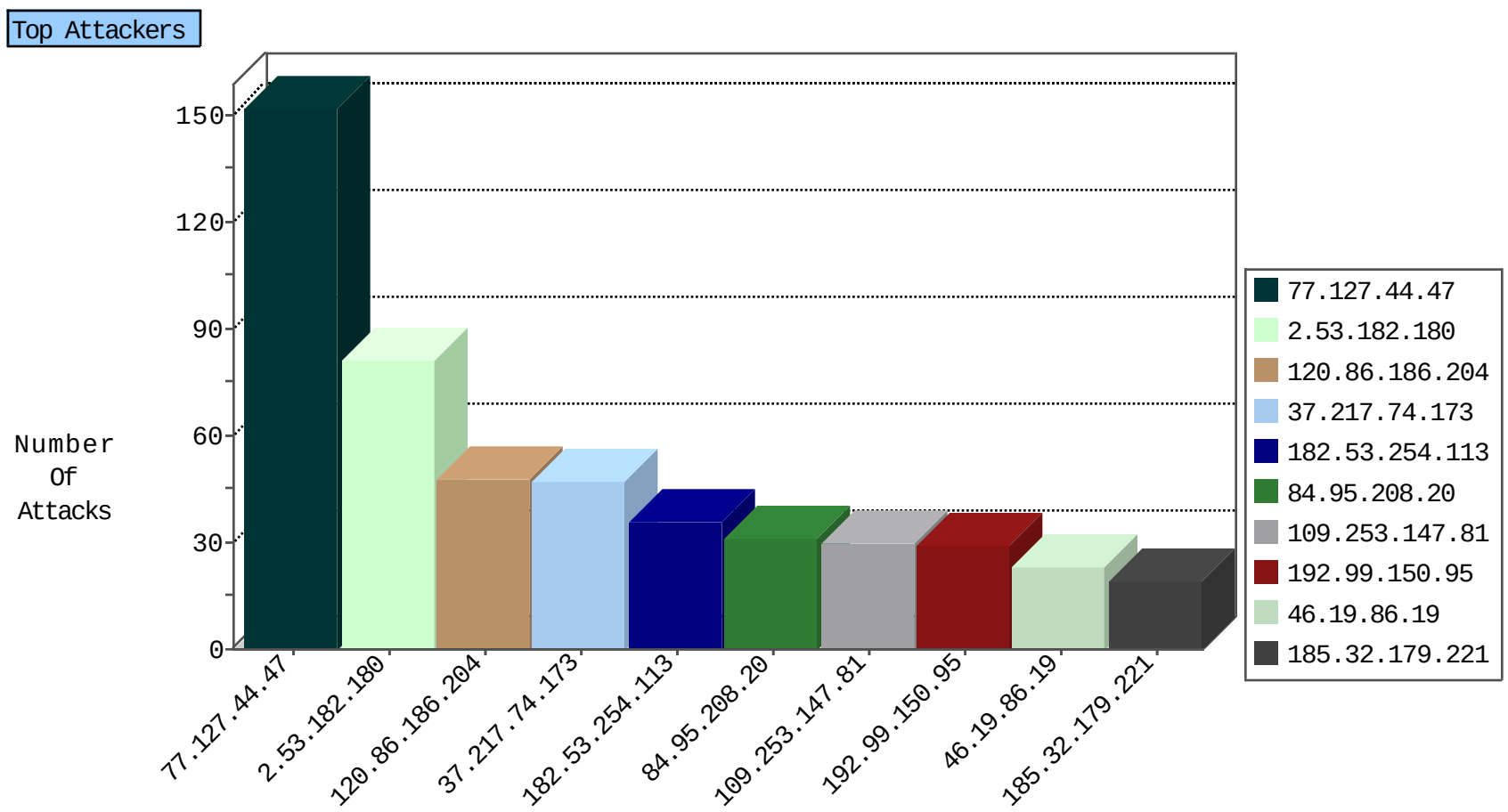
10-02-2016-08:04:05 to 10-02-2016-09:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-02-2016-08:04:05 to 10-02-2016-09:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.192.211	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	52
185.94.111.1	Russian Federation	147.237.76.201	e.atal.idf.il	Black List	drop	1
63.141.231.214	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
204.42.253.2	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1

10-02-2016-08:04:05 to 10-02-2016-09:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-02-2016-08:04:05 to 10-02-2016-09:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
14.152.59.11	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.81.71	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
106.38.241.106	147.237.72.156	China	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
62.150.255.205	147.237.76.34	Kuwait	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
46.249.82.10	147.237.76.196	Bulgaria	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
24.37.68.226	147.237.76.147	Canada	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.40.4.208	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.8.27	United Kingdom	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
62.150.255.205	147.237.76.34	Kuwait	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
46.249.82.10	147.237.76.196	Bulgaria	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
24.37.68.226	147.237.76.196	Canada	e.sviva.idf.il	ET SCAN Potential SSH Scan	1

10-02-2016-08:04:05 to 10-02-2016-09:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.217.74.173	Saudi Arabia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	47
109.253.147.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
80.246.133.60	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
182.53.254.113	Thailand	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.243.150.194	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
182.53.254.113	Thailand	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
80.246.130.171	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
185.32.179.221	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
192.99.150.95	Canada	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
46.19.85.84	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.19	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.99.150.95	Canada	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	6
46.19.85.84	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
182.53.254.113	Thailand	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
219.85.200.209	Taiwan	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
185.32.179.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
182.53.254.113	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
185.32.179.221	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
52.3.127.144	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
79.180.11.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
182.53.254.113	Thailand	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.19	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.253.146.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
109.201.138.238	Netherlands	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
192.99.150.95	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.251	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.99.150.95	Canada	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.99.150.95	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
202.79.21.58	Bangladesh	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.181	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.18.128	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
89.237.121.61	France	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
192.99.150.95	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.178	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
80.246.130.171	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.53.150.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.166.190.186	Netherlands	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
85.64.120.136	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
139.255.76.230	Indonesia	147.237.76.42	refuah.idf.il	SYN Attack		monitor	2
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	2
185.3.147.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
89.237.121.61	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.116.36.93	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2

10-02-2016-08:04:05 to 10-02-2016-09:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.127.44.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	151
2.53.182.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
120.86.186.204	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 120.86.186.204	Block	19
120.86.186.204	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 120.86.186.204	Block	15
37.46.39.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
79.178.227.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
120.86.186.204	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	7
120.86.186.204	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	6
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
2.55.53.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.128.185	Block	3
5.29.191.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
77.127.25.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	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
66.181.21.210	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/edim/library/generaldoc.asp	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
185.23.60.4	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	2
66.249.66.103	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.103	Block	2
5.97.217.162	Italy	147.237.0.19	madim.atal.idf.il	Unauthorized Method HEAD for /	Block	1
94.159.255.173	Israel	147.237.72.166	aka.idf.il	Unknown Parameter asm in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
66.249.64.107	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/109989	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	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
66.249.69.112	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/mobile/	Block	1
192.115.100.190	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/wars.asp	Block	1
157.55.39.43	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.64.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/שקו פית 8	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
66.249.73.188	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
77.127.44.47	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/mobile/templates/basket/basket.aspx	Block	1
172.92.4.43	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/sachar	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
85.64.36.220	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.78	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
120.86.186.204	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.asp	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/brothers/gallery/showpicture.asp	Block	1
77.138.138.99	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
66.249.65.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9237-he/refuah.aspx	Block	1
5.97.217.162	Italy	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /	Block	1
89.237.121.61	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.79.110	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/smalim/showbig.aspx	Block	1
66.249.64.21	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
185.32.179.45	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

10-02-2016-08:04:05 to 10-02-2016-09:04:05