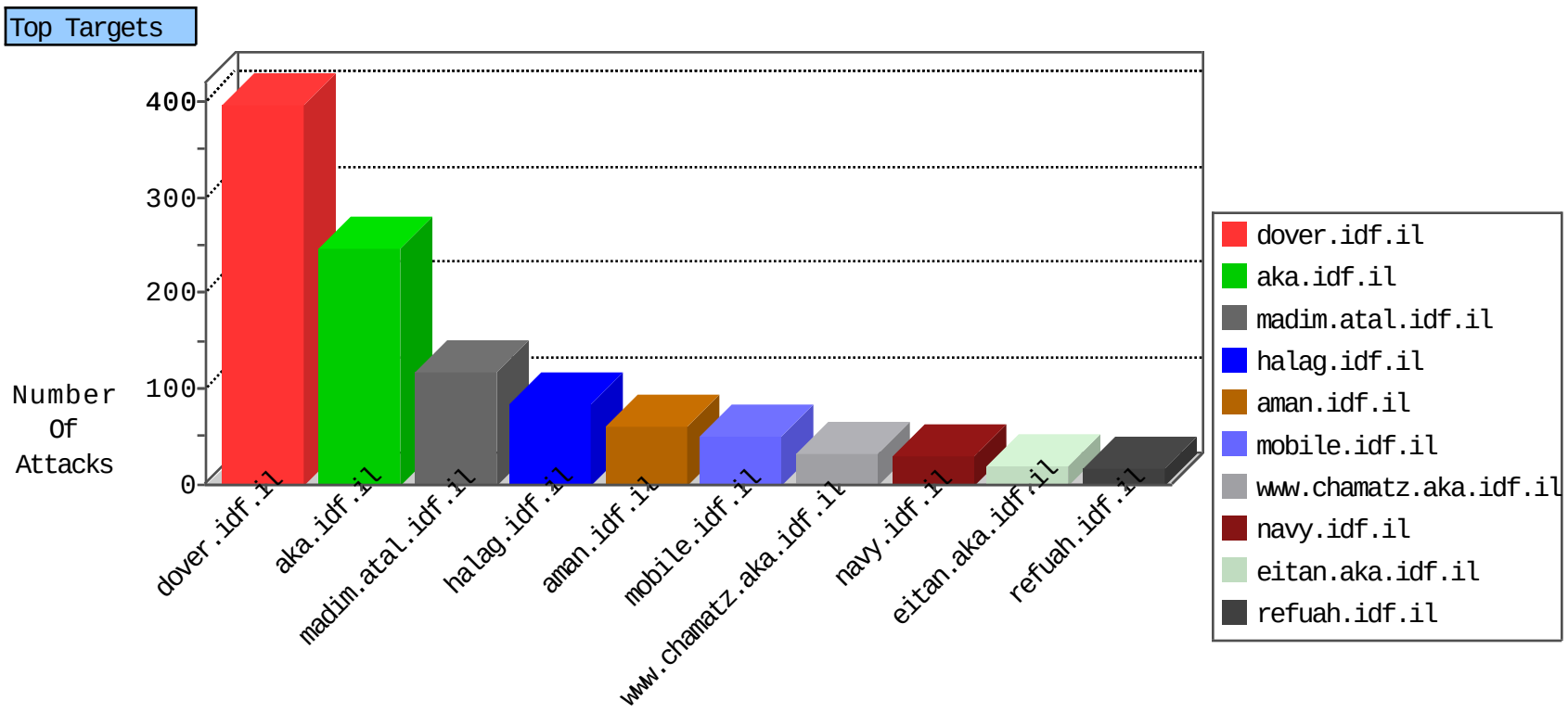
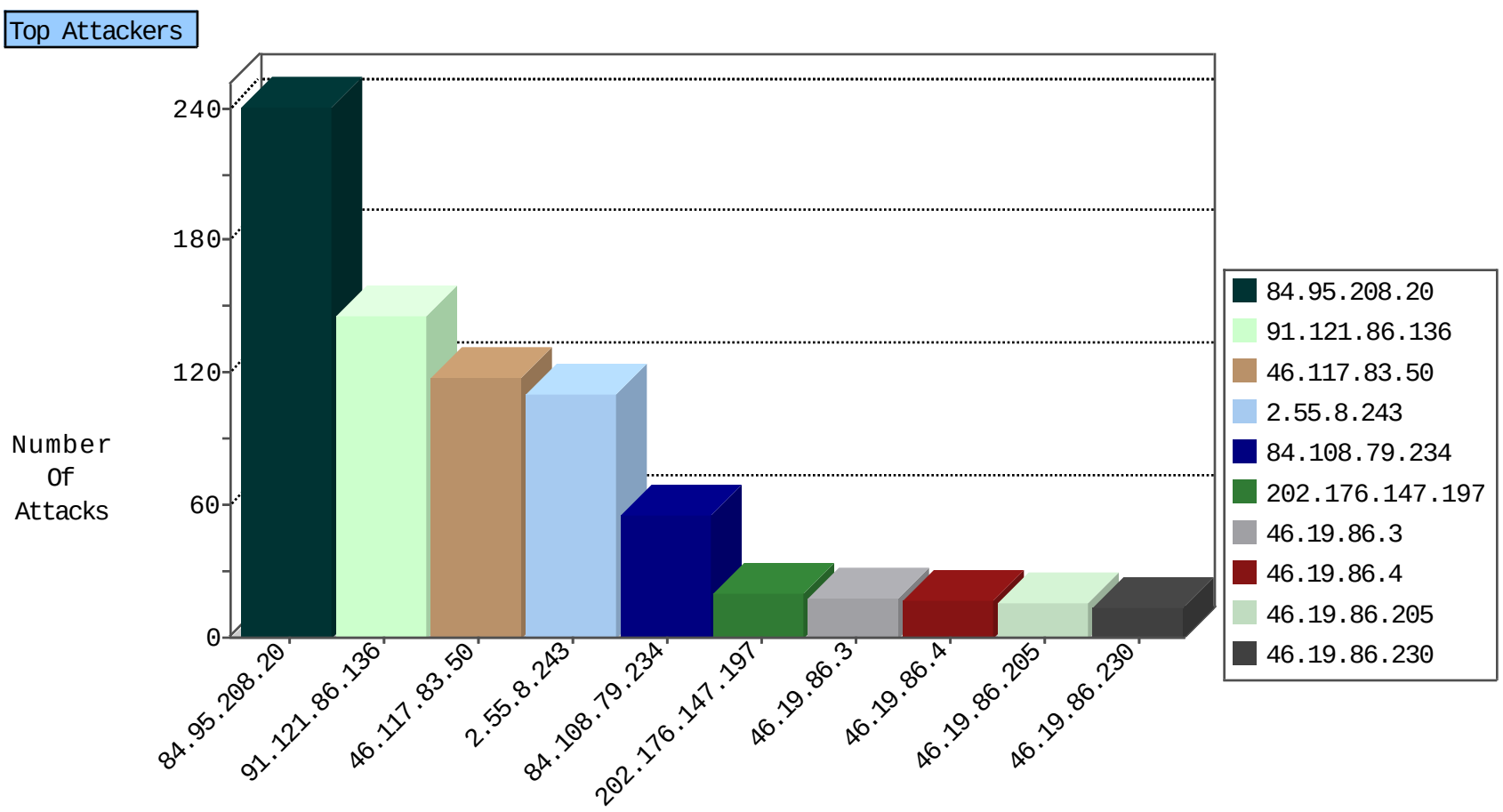
09-23-2016-12:04:04 to 09-23-2016-13:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-23-2016-12:04:04 to 09-23-2016-13:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
185.94.111.1	Russian Federation	147.237.76.201	e.atal.idf.il	Black List	drop	1
58.218.200.137	China	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
123.59.59.52	China	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1

09-23-2016-12:04:04 to 09-23-2016-13:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.121.86.136	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	126
91.121.86.136	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	9
69.30.210.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	9
91.121.86.136	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	6
91.121.86.136	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	4
176.9.10.227	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
176.9.10.227	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.254.121.188	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.197.163.195	United States	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Permit	2
151.80.31.169	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

09-23-2016-12:04:04 to 09-23-2016-13:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.250.190.142	147.237.77.216	Canada	dover.idf.il	Xenu Link Sleuth User Agent	2
52.42.115.117	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
163.172.129.15	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.28.189	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.225	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
116.71.128.85	147.237.8.24	Pakistan	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.77.233	Ukraine	atal.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.50	147.237.77.233	Ukraine	atal.idf.il	ET SCAN NMAP -f -sS	1
66.249.79.2	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
185.93.185.10	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.218.200.137	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
52.42.115.117	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
183.60.48.25	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
52.42.115.117	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -f -sS	1
163.172.129.15	147.237.76.39	United Kingdom	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
41.215.36.46	147.237.76.196	Kenya	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.187.89	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
109.60.153.178	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.77.233	Ukraine	atal.idf.il	ET SCAN NMAP -sS window 2048	1
77.127.41.234	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
211.149.197.148	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1

09-23-2016-12:04:04 to 09-23-2016-13:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.117.83.50	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	62
84.108.79.234	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
46.117.83.50	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	25
202.176.147.197	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
46.19.86.3	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.205	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	13
62.0.197.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.4	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.117.83.50	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
199.187.241.236	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.83.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.4	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.122.154.42	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.254	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
27.251.64.154	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.215	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.93.85	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
89.108.144.115	Lebanon	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
80.246.136.43	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.117.83.50	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	5
46.19.86.215	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.14	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
93.173.67.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
66.249.93.87	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.142.209.156	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
66.249.76.2	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.199.251.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.32.179.149	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
141.226.218.90	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.117.83.50	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.68.13.33	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.205	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.117.83.50	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.3.147.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.117.83.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
46.19.85.154	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.15.48	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.253.242.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.246.139.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
79.181.116.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2

09-23-2016-12:04:04 to 09-23-2016-13:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.8.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	93
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	80
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	18
77.138.174.95	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaireend.aspx	Block	13
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	12
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	8
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
66.249.76.30	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.76.30	Block	4
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
46.19.86.164	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	Distributed PHP Attempt	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
79.178.25.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.31	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.76.31	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.111.65.145	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
109.253.211.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.254	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method uage: in URL he-il	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
84.108.79.234	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
157.55.39.108	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
46.116.86.52	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/sachar/undefined	Block	1
79.179.28.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.79.53	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/webservices/wscity.asmx	Block	1
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
84.109.51.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.215	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
77.138.200.77	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
180.76.15.34	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
66.249.76.31	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1744	Block	1
46.117.83.50	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
37.26.147.207	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/null	Block	1
69.197.163.195	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8746-he/refuah.aspx	Block	1
46.19.86.254	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version	Block	1
77.138.234.56	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
192.198.151.43	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/inner.asp	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.106	Block	1
46.121.213.149	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
37.162.206.171	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
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
46.19.86.254	Israel	147.237.76.42	refuah.idf.il	Malformed URL he-il	Block	1
79.177.29.180	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
213.151.35.221	Israel	147.237.72.156	aman.idf.il	Double URL Encoding - parameter: rdfrom in www.aman.idf.il/	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/reserve/	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/homepage/piwik.php	Block	1
66.102.9.3	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

09-23-2016-12:04:04 to 09-23-2016-13:04:04