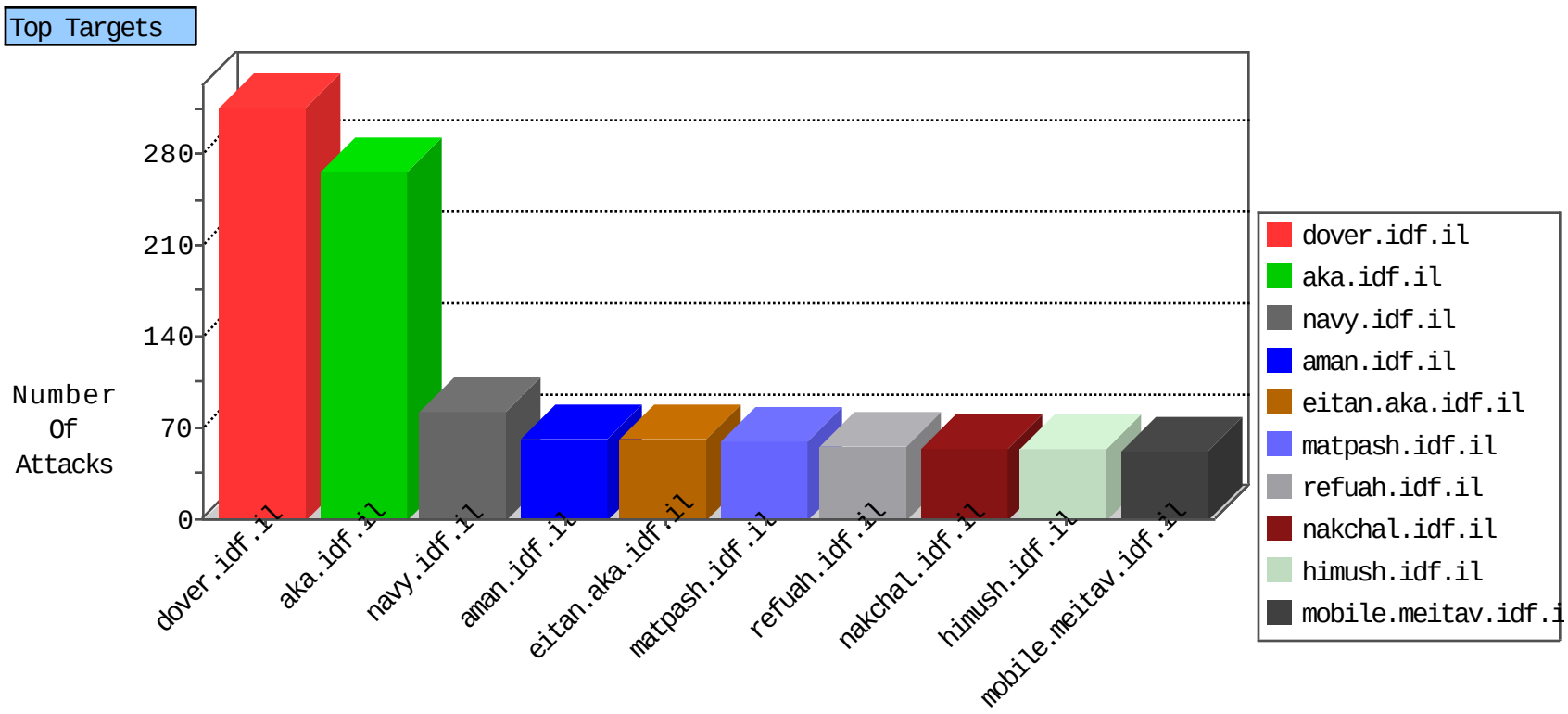
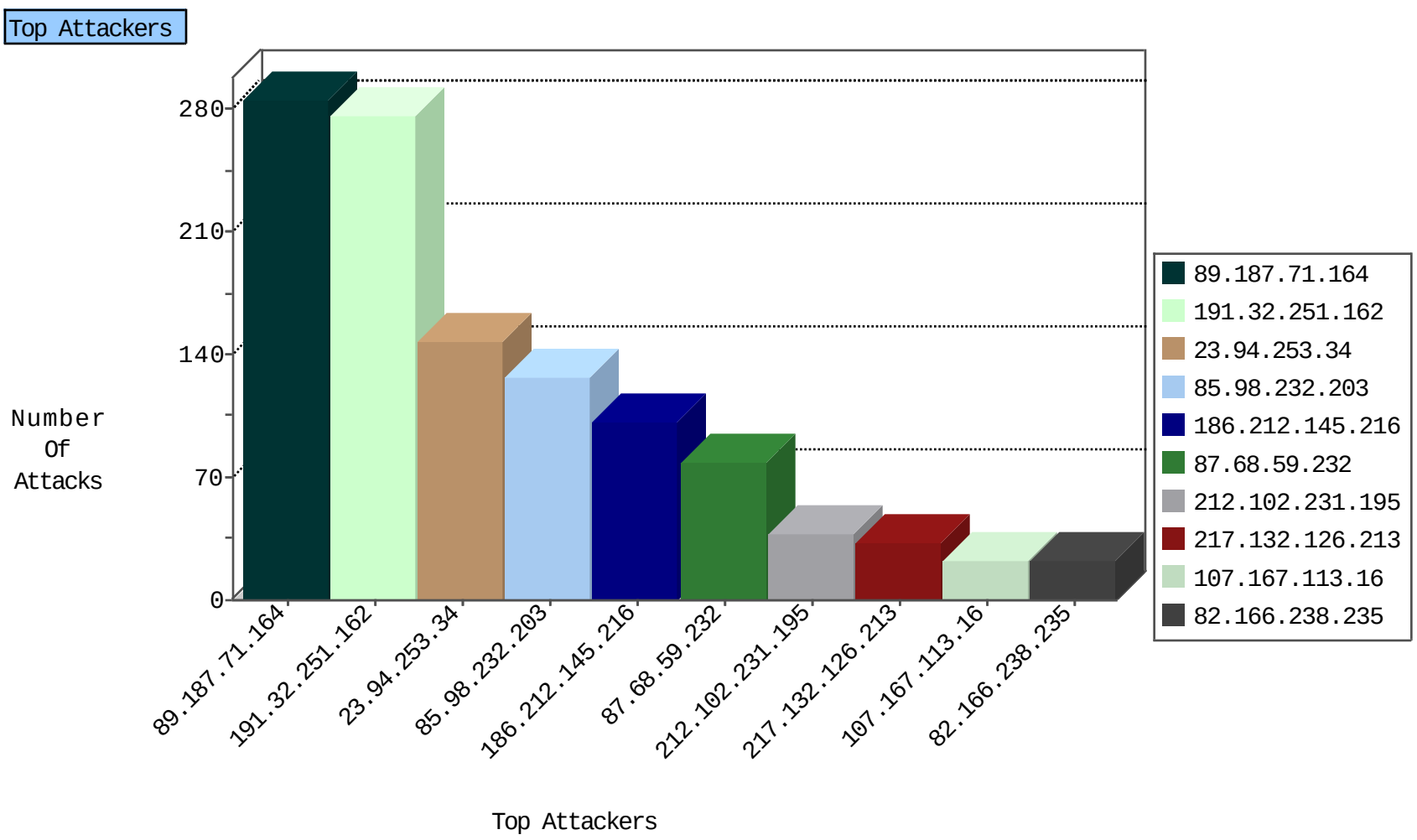
09-08-2016-23:04:09 to 09-09-2016-00:04:09

IDF Under Attack
Daily Report





09-08-2016-23:04:09 to 09-09-2016-00:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.67.1.206	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
123.59.59.52	China	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
149.202.57.201	France	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
149.202.57.201	France	147.237.76.200	eitan.aka.idf.il	Black List	drop	1

09-08-2016-23:04:09 to 09-09-2016-00:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-08-2016-23:04:09 to 09-09-2016-00:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
59.67.64.13	147.237.77.121	China	e.navy.idf.il	GPL SCAN nmap TCP	2
109.60.153.178	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.94.142	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.64.107	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
196.47.173.21	147.237.76.200	Cote D'Ivoire	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.208.193	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.162	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.161	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
116.31.116.12	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.195	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.149	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.76.200	Cote D'Ivoire	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.66	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.208.193	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.135	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
189.161.173.106	147.237.0.200	Mexico	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
180.97.106.162	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
165.215.209.15	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
116.31.116.12	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1

09-08-2016-23:04:09 to 09-09-2016-00:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.98.232.203	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	97
85.98.232.203	Turkey	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	28
87.68.59.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
87.68.59.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27
87.68.59.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	25
107.167.113.16	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
217.132.126.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
23.94.253.34	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
23.94.253.34	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
23.94.253.34	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
23.94.253.34	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
23.94.253.34	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
23.94.253.34	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
23.94.253.34	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
23.94.253.34	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
89.187.71.164	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
93.172.212.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
89.187.71.164	United Kingdom	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
89.187.71.164	United Kingdom	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
89.187.71.164	United Kingdom	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
89.187.71.164	United Kingdom	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
191.32.251.162	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
89.187.71.164	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
191.32.251.162	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
89.187.71.164	United Kingdom	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
89.187.71.164	United Kingdom	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
89.187.71.164	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
191.32.251.162	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
89.187.71.164	United Kingdom	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
191.32.251.162	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
89.187.71.164	United Kingdom	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
191.32.251.162	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
89.187.71.164	United Kingdom	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
191.32.251.162	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
217.132.126.213	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	13
89.187.71.164	United Kingdom	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
191.32.251.162	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
89.187.71.164	United Kingdom	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
191.32.251.162	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
191.32.251.162	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
89.187.71.164	United Kingdom	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
191.32.251.162	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
89.187.71.164	United Kingdom	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
191.32.251.162	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
89.187.71.164	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
191.32.251.162	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
89.187.71.164	United Kingdom	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
89.187.71.164	United Kingdom	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
191.32.251.162	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
191.32.251.162	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12

09-08-2016-23:04:09 to 09-09-2016-00:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.168.139	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.168.139	Block	4
109.253.146.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
185.32.179.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
89.139.122.192	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
77.138.141.148	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/rights/asp/info.asp	Block	2
46.116.98.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
87.69.168.139	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	2
79.178.244.107	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$txtPassword in www.aka.idf.il/main/giyus/faq.aspx	None	1
66.249.93.83	Israel	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
212.199.218.246	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.207	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method Accept-Language: in URL en-gb,en	Block	1
109.67.153.64	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/miluim/	Block	1
79.178.244.107	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$txtSearch in www.aka.idf.il/main/giyus/updateuserdetails.aspx	None	1
66.249.93.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/admin	Block	1
192.116.177.130	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
87.69.168.139	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.69.168.139	Block	1
77.138.237.100	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
216.244.66.231	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
79.179.6.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.93.87	Israel	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
46.19.86.207	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
198.161.119.4	Canada	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 198.161.119.4 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
77.138.251.201	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
66.102.6.23	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
124.73.6.250	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1694-11699-he/cogat.aspx/trackback/	Block	1
85.64.144.158	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.93.87	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin	Block	1
46.19.86.207	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
198.161.119.4	Canada	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.178.21.104	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	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
157.55.39.253	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
87.69.162.24	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
77.138.9.5	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx	Block	1
46.19.86.207	Israel	147.237.77.216	dover.idf.il	Malformed URL en-gb,en;q=0.8,en-us;q=0.6,he;q=0.4	Block	1
204.79.180.103	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
95.86.86.3	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1

09-08-2016-23:04:09 to 09-09-2016-00:04:09