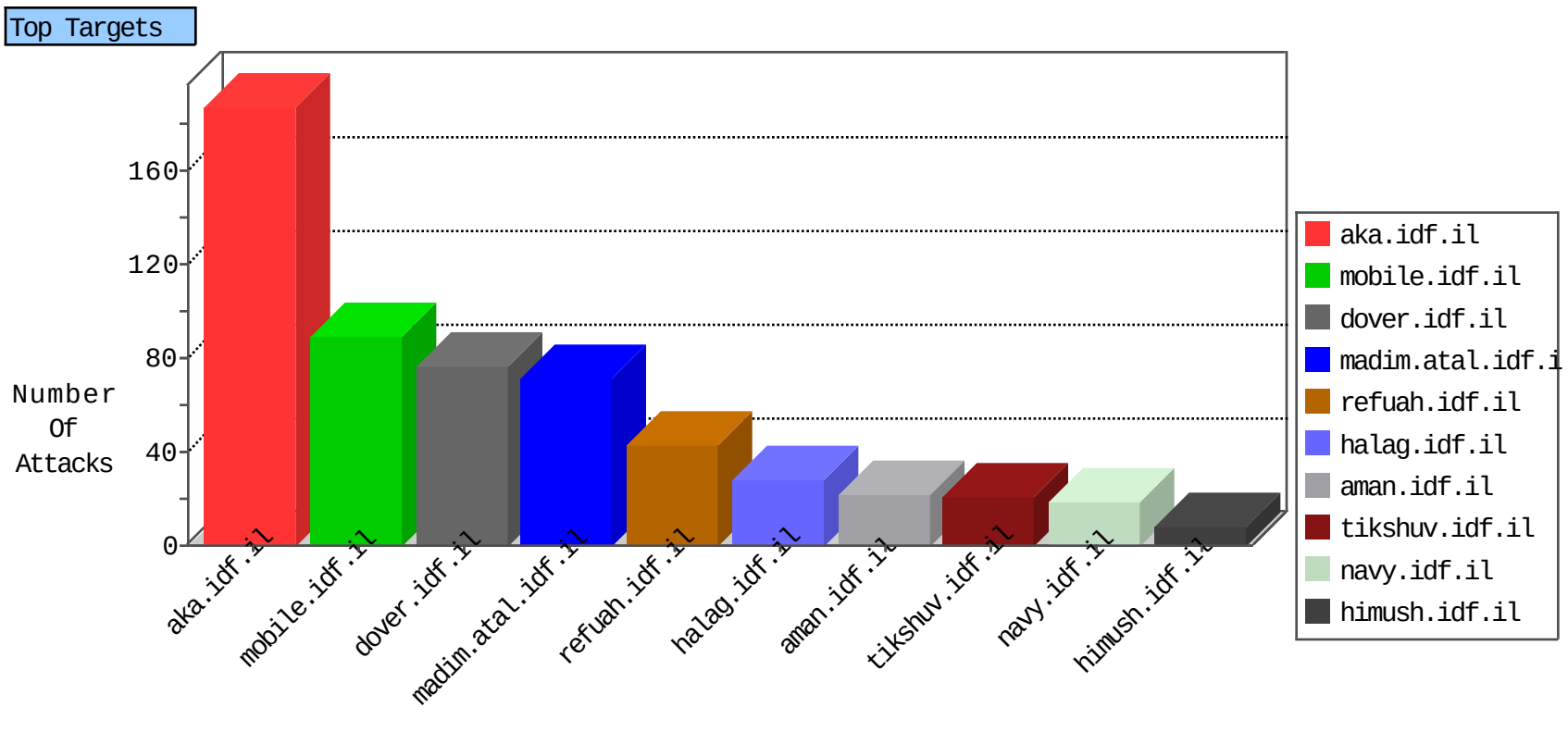
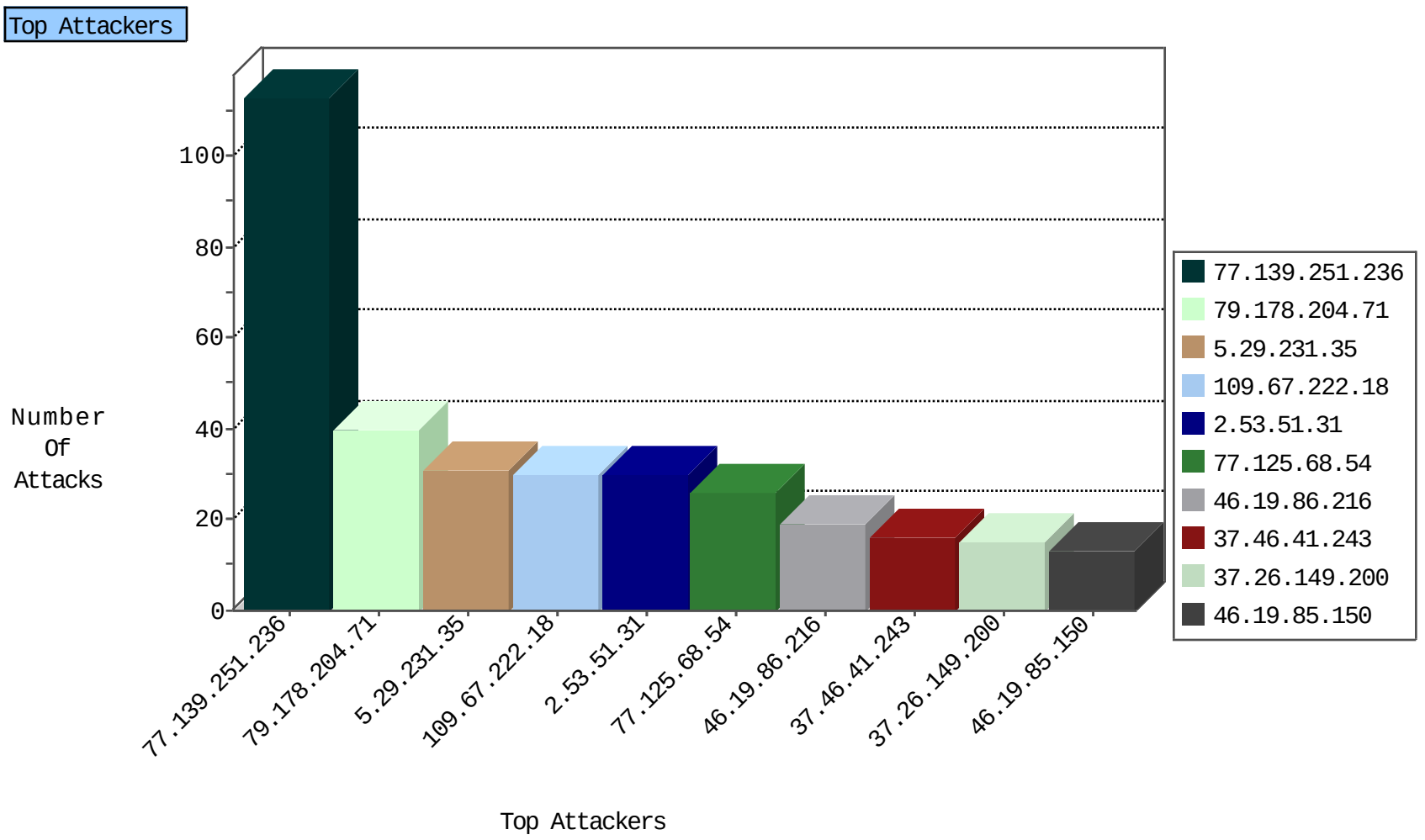
09-23-2016-20:04:01 to 09-23-2016-21:04:01

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-23-2016-20:04:01 to 09-23-2016-21:04:01

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	SYN Flood out of context	drop	13
37.26.146.251	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.53.140.125	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
142.54.174.86	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
46.19.85.123	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
203.87.133.144	Philippines	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
71.19.248.195	Canada	147.237.76.30	himush.idf.il	Black List	drop	1
137.226.113.7	Germany	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
45.32.193.80	Netherlands	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1

09-23-2016-20:04:01 to 09-23-2016-21:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
92.45.244.24	Turkey	147.237.72.166	aka.idf.il	2023: HTTP: Cross Site Scripting in GET Request	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-23-2016-20:04:01 to 09-23-2016-21:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.226.40.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.60.153.178	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
92.45.244.24	147.237.72.166	Turkey	aka.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scriptin Attempt	1
221.226.31.210	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
61.178.42.242	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
221.6.32.82	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
58.218.200.137	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.26.148.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.169.150	147.237.0.15	United Kingdom	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
115.47.12.162	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
221.226.31.210	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
221.6.32.82	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
61.178.42.242	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
210.212.207.80	147.237.0.15	India	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.183.223.228	147.237.0.35	Latvia	akaws.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.55.151.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN NMAP -sS window 1024	1
115.47.12.162	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1

09-23-2016-20:04:01 to 09-23-2016-21:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.51.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.67.222.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
77.139.251.236	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
79.178.204.71	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
77.139.251.236	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
77.139.251.236	France	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	24
77.139.251.236	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
37.46.41.243	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
37.26.149.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
77.139.251.236	France	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
176.13.230.67	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.216	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
213.113.254.172	Sweden	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.85.150	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.86	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
31.154.81.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.150	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.179.14.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
79.178.204.71	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
213.57.195.190	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
84.94.182.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
79.178.102.130	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
208.54.87.252	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
79.178.204.71	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.178.204.71	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
79.182.0.114	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.123	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.216	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
37.26.148.218	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.179.14.172	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
84.94.182.87	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
94.230.86.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.176	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.113	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
91.209.51.22	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
46.19.86.216	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.94.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
5.102.242.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.18	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
91.209.51.22	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
84.108.94.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
31.154.81.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
188.120.148.19	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
92.45.244.24	Turkey	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
5.29.114.35	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.26.147.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

09-23-2016-20:04:01 to 09-23-2016-21:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.231.35	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/templates/catalog/catalog.aspx	Block	31
77.125.68.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
2.55.182.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
80.246.138.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.57.254.39	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/default.aspx/modiin/default.aspx	Block	2
87.68.17.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
1.22.113.79	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
147.9.209.165	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
79.179.14.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.8.215	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
194.187.170.102	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il./robots.txt	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
176.228.151.248	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/he/navy.aspx	Block	1
79.181.202.98	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	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
109.64.44.170	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
180.76.15.160	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	1
66.249.65.160	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1437-he/atal.aspx	Block	1
213.113.254.172	Sweden	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.66.22.242	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 109.66.22.242 (Open Mode)	None	1
77.138.199.134	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunpersonalquestionnaire.aspx	Block	1
37.46.41.243	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
185.27.106.103	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.65.182	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/5/695.doc	Block	1
109.66.22.242	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.178.204.71	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.19.86.216	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
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
92.45.244.24	Turkey	147.237.72.166	aka.idf.il	Unknown Parameter %3script%3ealert(/MySQLError/)%3c/script%3e in www.aka.idf.il/giyus/general/	None	1
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2922.pdf	Block	1

09-23-2016-20:04:01 to 09-23-2016-21:04:01