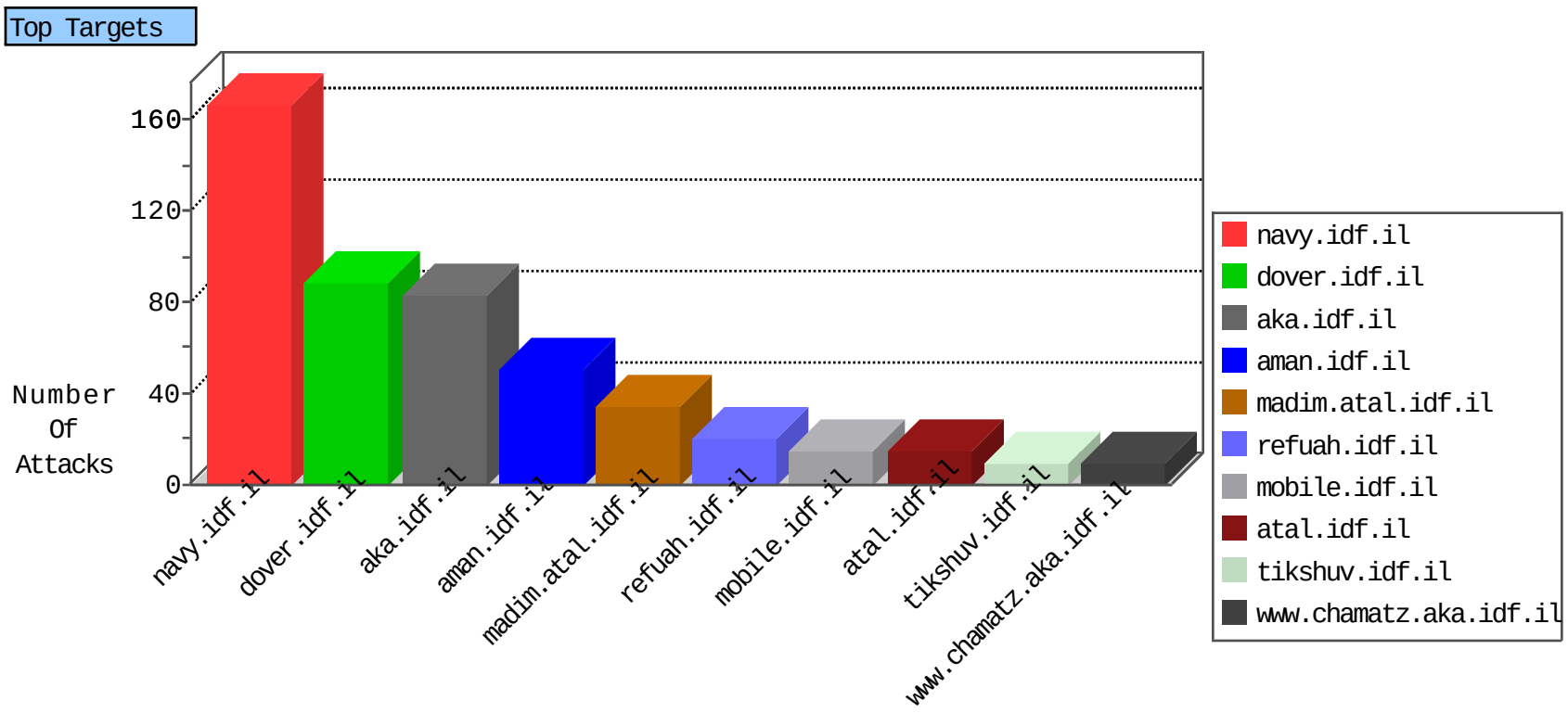
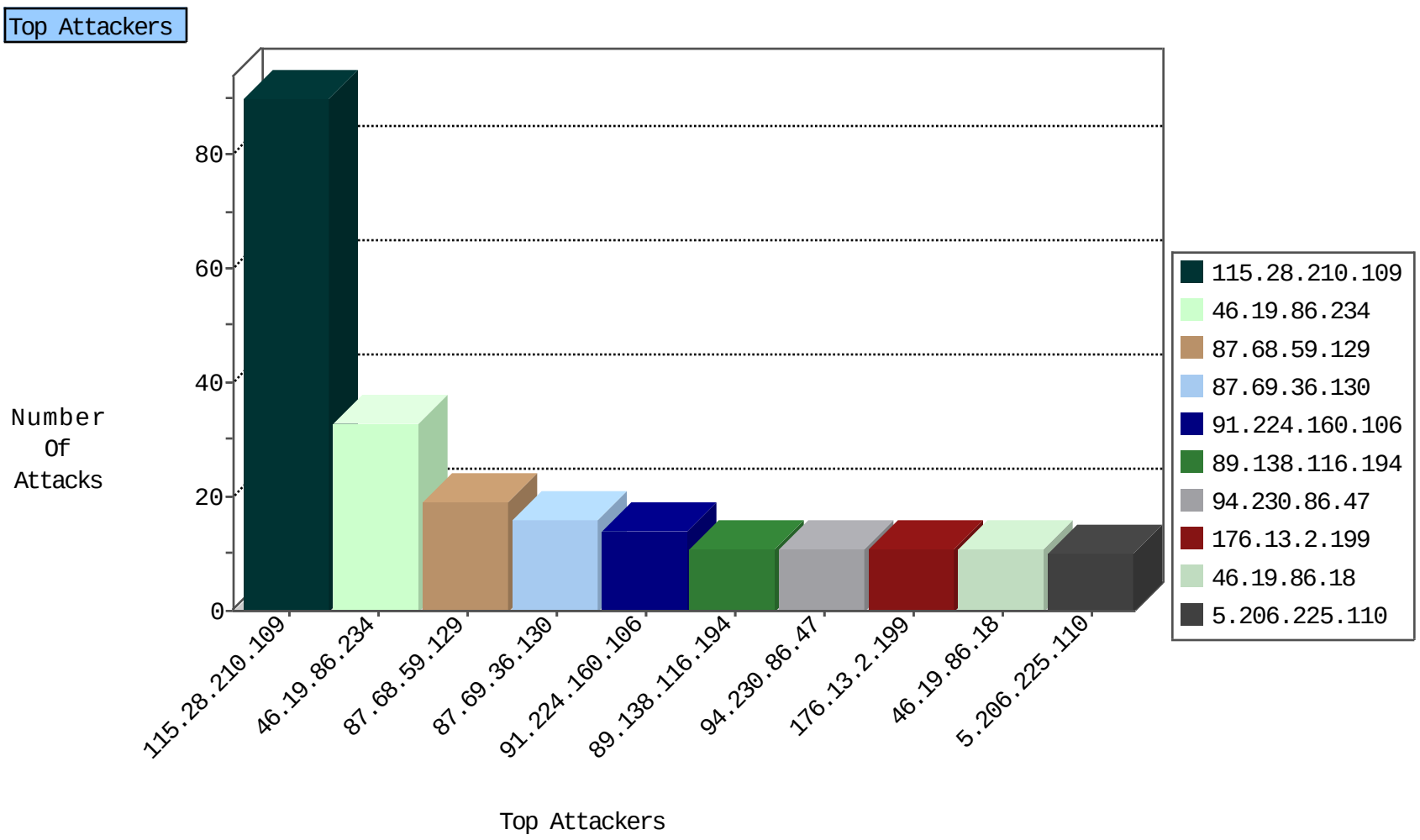
09-09-2016-16:04:07 to 09-09-2016-17:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-09-2016-16:04:07 to 09-09-2016-17:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.105.139	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
89.187.217.74	Lebanon	147.237.77.61	e.cogat.idf.il	L4 Source or Dest Port Zero	drop	1
185.94.111.1	Russian Federation	147.237.76.86	navy.idf.il	Black List	drop	1
212.34.23.151	Jordan	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1
79.178.26.193	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-09-2016-16:04:07 to 09-09-2016-17:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-09-2016-16:04:07 to 09-09-2016-17:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	4
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
96.126.126.142	147.237.77.216	United States	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
91.224.160.106	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	2
84.93.84.77	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
91.224.160.106	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
194.58.37.44	147.237.77.74	Russian Federation	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
163.172.129.15	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.160.106	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.77.178	United Kingdom	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.160.106	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.77.121	United Kingdom	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
52.166.130.115	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
52.166.130.115	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential SSH Scan	1
208.73.143.36	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.160.106	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.160.106	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.77.176	United Kingdom	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.65.169.33	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	1
52.166.130.115	147.237.77.233	United States	atal.idf.il	ET SCAN Potential SSH Scan	1
93.158.203.168	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
52.166.130.115	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	1

09-09-2016-16:04:07 to 09-09-2016-17:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
115.28.210.109	China	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
115.28.210.109	China	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	21
115.28.210.109	China	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	19
115.28.210.109	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
115.28.210.109	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
87.68.59.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
89.138.116.194	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
176.13.2.199	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.176.76.78	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
87.68.59.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
87.69.36.130	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
94.230.86.47	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.18	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	9
93.172.12.148	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
87.69.36.130	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
37.26.148.136	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.95	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.132.15	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.7	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.137.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
138.246.253.19	Germany	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
84.94.113.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
178.134.63.55	Georgia	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
77.124.247.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
138.246.253.19	Germany	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
185.11.146.59	Netherlands	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
37.46.38.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.7	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
85.65.24.18	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
141.226.217.228	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.11.146.59	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.206.225.110	Portugal	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.143	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
85.65.24.18	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.206.225.110	Portugal	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
46.19.86.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.143.164.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
95.86.69.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.53	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
79.180.250.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.75	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
104.197.105.144	United States	147.237.76.42	refuah.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
5.206.225.110	Portugal	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
176.13.13.230	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.148.180	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

09-09-2016-16:04:07 to 09-09-2016-17:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
79.179.50.204	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	10
212.199.218.246	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	6
46.120.53.135	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	3
176.13.2.199	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
89.139.97.38	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
84.108.108.80	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
94.230.86.47	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
79.178.194.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/57056.pdf&ved=0ahukewj88mpmt6fmahuc_iwkhwntar4qfggdmai&usg=afqjcnf1yolugsboijiblzxiye0gplabcg&sig2=sljt3vnb9hu32rwuqzye5w	Block	2
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily-statistics/english/	Block	1
46.116.53.164	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
89.138.116.194	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.66.24	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/6/1066.pdf	Block	1
96.126.126.142	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.108.47.91	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
46.116.69.185	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.116.69.185	Block	1
185.32.179.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
79.180.93.132	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.66.107	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/m/main/giyus/userdetails/updateuserdetails.aspx	Block	1
46.29.250.242	Sweden	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
96.126.126.142	United States	147.237.77.216	dover.idf.il	Unauthorized Method OPTIONS for /	Block	1
66.249.76.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	1
46.116.69.185	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus=	Block	1
197.15.236.215	Tunisia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	1
2.53.38.63	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.180.93.132	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.66.232	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.29.250.242	Sweden	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/wp/wp-login.php	Block	1
109.64.100.31	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
85.65.202.246	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
77.139.48.150	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
96.126.126.142	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
2.53.48.113	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
82.81.10.32	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
46.112.148.35	Poland	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
85.65.202.246	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 85.65.202.246	Block	1
213.6.75.142	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/dover.aspx/sql	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
96.126.126.142	United States	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 96.126.126.142 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
31.168.185.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.94.113.216	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/size220x0/sip_storage	Block	1

09-09-2016-16:04:07 to 09-09-2016-17:04:07