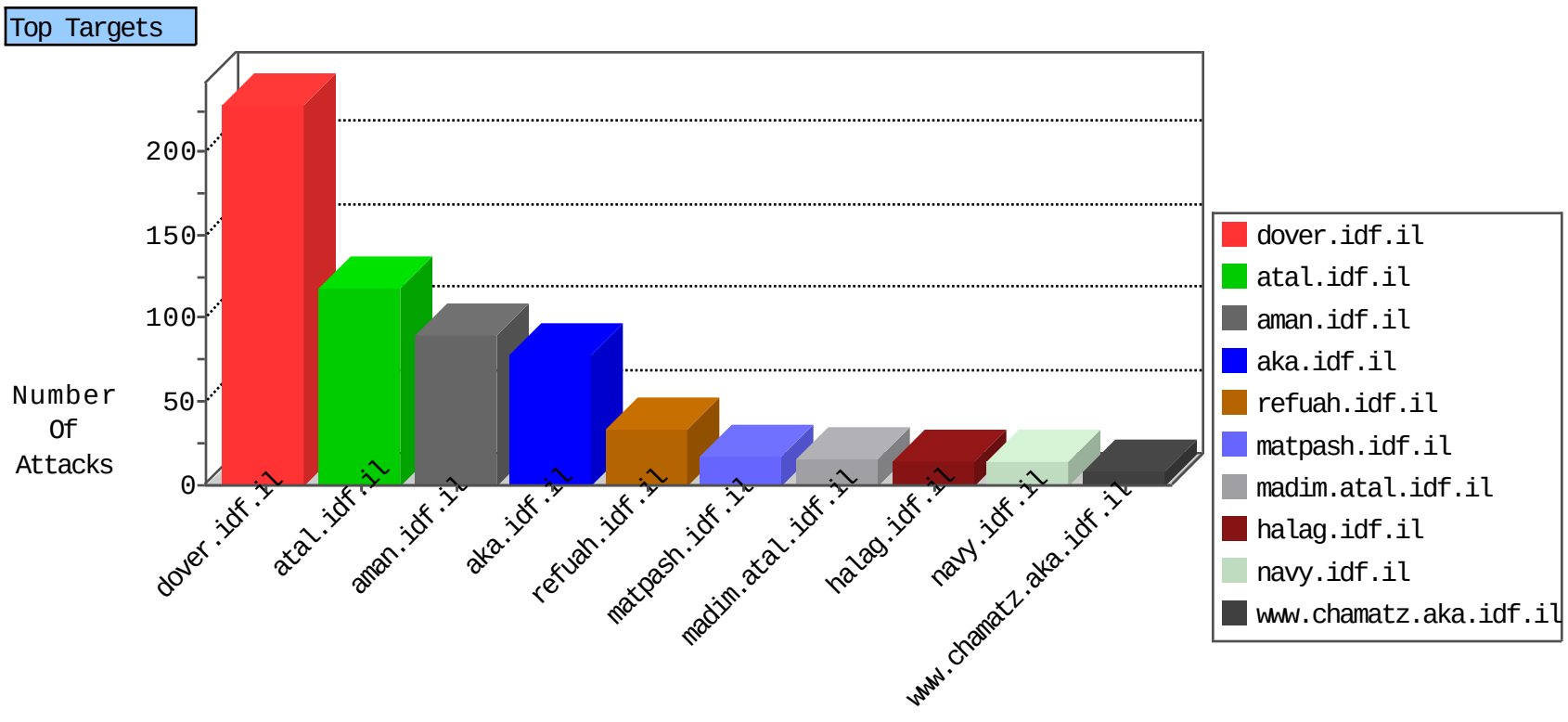
10-04-2016-16:04:09 to 10-04-2016-17:04:09

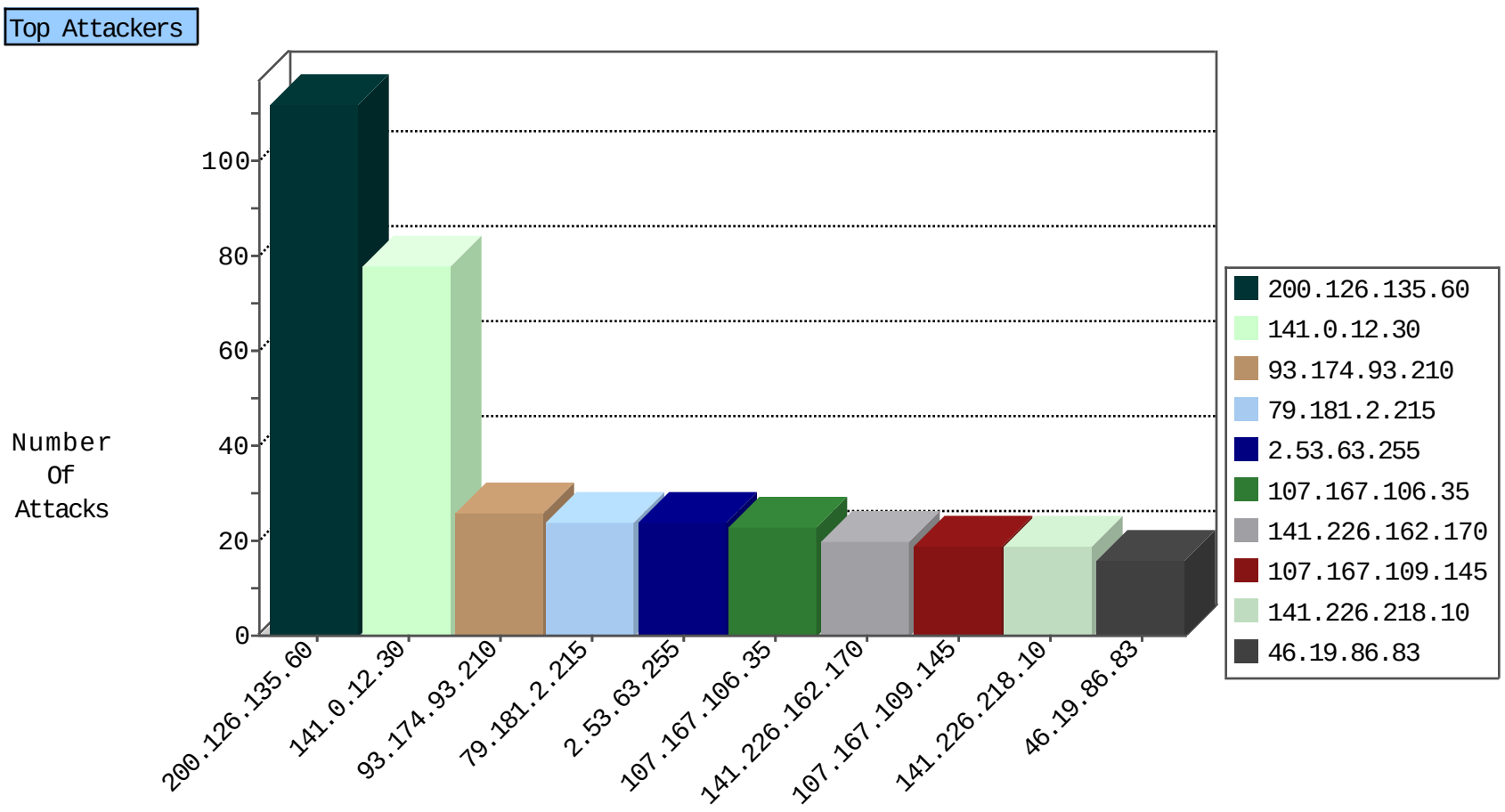
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-04-2016-16:04:09 to 10-04-2016-17:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.249.0.134	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
93.174.93.210	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
221.229.172.116	China	147.237.76.31	nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
93.174.93.210	Netherlands	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
93.174.93.210	Netherlands	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
79.177.175.132	Israel	147.237.72.156	aman.idf.il	Black List	drop	1

10-04-2016-16:04:09 to 10-04-2016-17:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.111.70	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
89.40.28.7	Romania	147.237.77.216	dover.idf.i	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	1
89.40.28.7	Romania	147.237.77.216	dover.idf.i	22095: HTTP: Joomla Image Manager folderRename Security Bypass Vulnerability	Block	1

10-04-2016-16:04:09 to 10-04-2016-17:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
89.40.28.7	147.237.77.216	Romania	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.154.184.122	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
109.253.141.64	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
109.236.86.32	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.39.188	147.237.76.42	France	refuah.idf.il	ET SCAN Potential SSH Scan	1
109.236.86.32	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.154.39.188	147.237.76.34	France	yohalan.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.77.61	Canada	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
195.154.39.188	147.237.0.33	France	idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
54.91.134.228	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
151.11.201.3	147.237.72.166	Italy	aka.idf.il	ET SCAN NMAP -sS window 3072	1
151.11.201.3	147.237.72.166	Italy	aka.idf.il	ET SCAN NMAP -f -sS	1
111.23.12.94	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
201.197.110.130	147.237.76.39	Costa Rica	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.236.86.32	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.154.39.188	147.237.77.216	France	dover.idf.il	ET SCAN Potential SSH Scan	1
109.236.86.32	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.154.39.188	147.237.76.38	France	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.77.61	Canada	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
195.154.39.188	147.237.72.167	France	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.0.15	Canada	kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
195.154.39.188	147.237.0.17	France	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.105	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
163.172.129.15	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
27.25.118.223	147.237.76.201	China	e.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
151.11.201.3	147.237.72.166	Italy	aka.idf.il	ET SCAN NMAP -sS window 2048	1
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	1

10-04-2016-16:04:09 to 10-04-2016-17:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
200.126.135.60	Argentina	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	109
141.0.12.30	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	78
107.167.106.35	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
107.167.109.145	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
141.226.218.10	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
79.181.2.215	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
79.181.2.215	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
141.226.162.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
141.226.162.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.253.159.100	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
2.53.63.255	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
71.207.197.175	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.63.255	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
89.40.28.7	Romania	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
61.3.79.148	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.211.53	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
176.13.21.70	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.205	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
79.178.27.36	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
79.178.27.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
129.45.125.34	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
94.14.154.155	United Kingdom	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
2.53.63.255	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
217.132.98.45	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.53.63.255	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
93.174.93.210	Netherlands	147.237.77.234	halag.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
37.46.38.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
85.64.71.250	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
207.46.13.58	United States	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.211	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
93.174.93.210	Netherlands	147.237.77.233	atal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
46.19.86.83	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
176.13.238.2	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
31.154.81.78	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.83	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.127.90.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.174.93.210	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
2.53.1.182	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.178.70.220	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.83	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
109.67.48.240	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
93.174.93.210	Netherlands	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.32.179.217	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.127	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.67	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.83	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.253.132.173	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
141.226.218.10	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	2

10-04-2016-16:04:09 to 10-04-2016-17:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.132.148.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.85.28	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	6
99.227.116.148	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	3
37.142.11.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.143.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.27.106.111	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	2
77.138.170.106	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/faq.aspx	Block	2
157.55.39.208	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
77.139.21.150	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	1
5.29.247.5	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
178.34.162.253	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
77.139.66.39	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/drushim	Block	1
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
130.60.4.12	Switzerland	147.237.77.74	law.idf.il	Parameter Type Violation SearchText in www.law.idf.il/657-en/patzar.aspx	Block	1
66.249.93.209	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catIdF in www.aka.idf.il/main/giyus/general.aspx	None	1
37.142.3.146	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/reset.css	Block	1
79.178.83.198	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.127	Israel	147.237.76.86	navy.idf.il	Malformed URL	Block	1
141.226.218.10	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
74.101.195.157	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/tizmoret/gallery/	Block	1
200.126.135.60	Argentina	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
79.181.140.101	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.19.86.127	Israel	147.237.76.86	navy.idf.il	Unknown HTTP Request Method facebook.katana in URL	Block	1
2.53.141.114	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
144.76.236.183	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
41.107.51.39	Algeria	147.237.77.216	dover.idf.il	Unauthorized Method POST for 147.237.77.216/	Block	1
82.166.103.58	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$passwordUpdate$txtPasswordRepeat in www.aka.idf.il/main/giyus/faq.aspx	None	1
66.249.66.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1

10-04-2016-16:04:09 to 10-04-2016-17:04:09