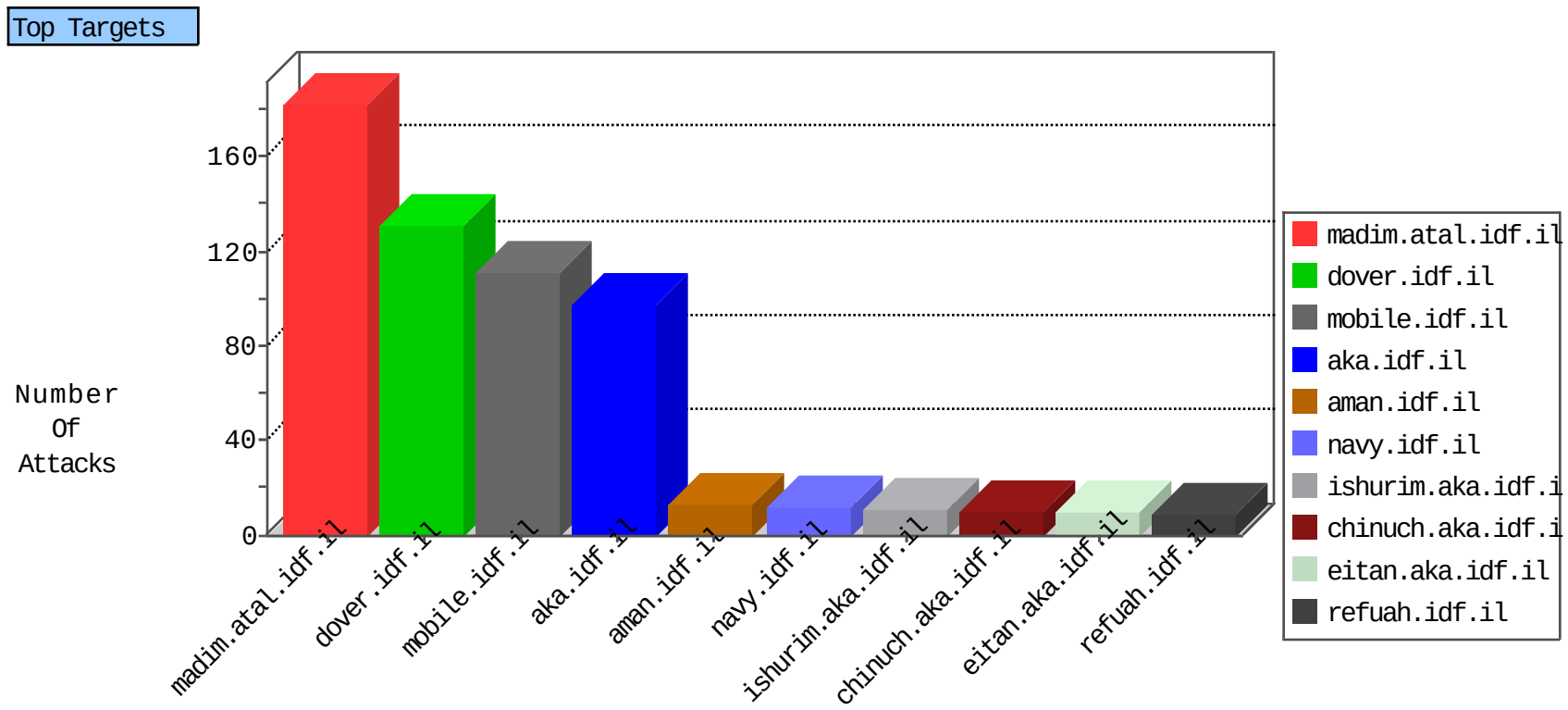
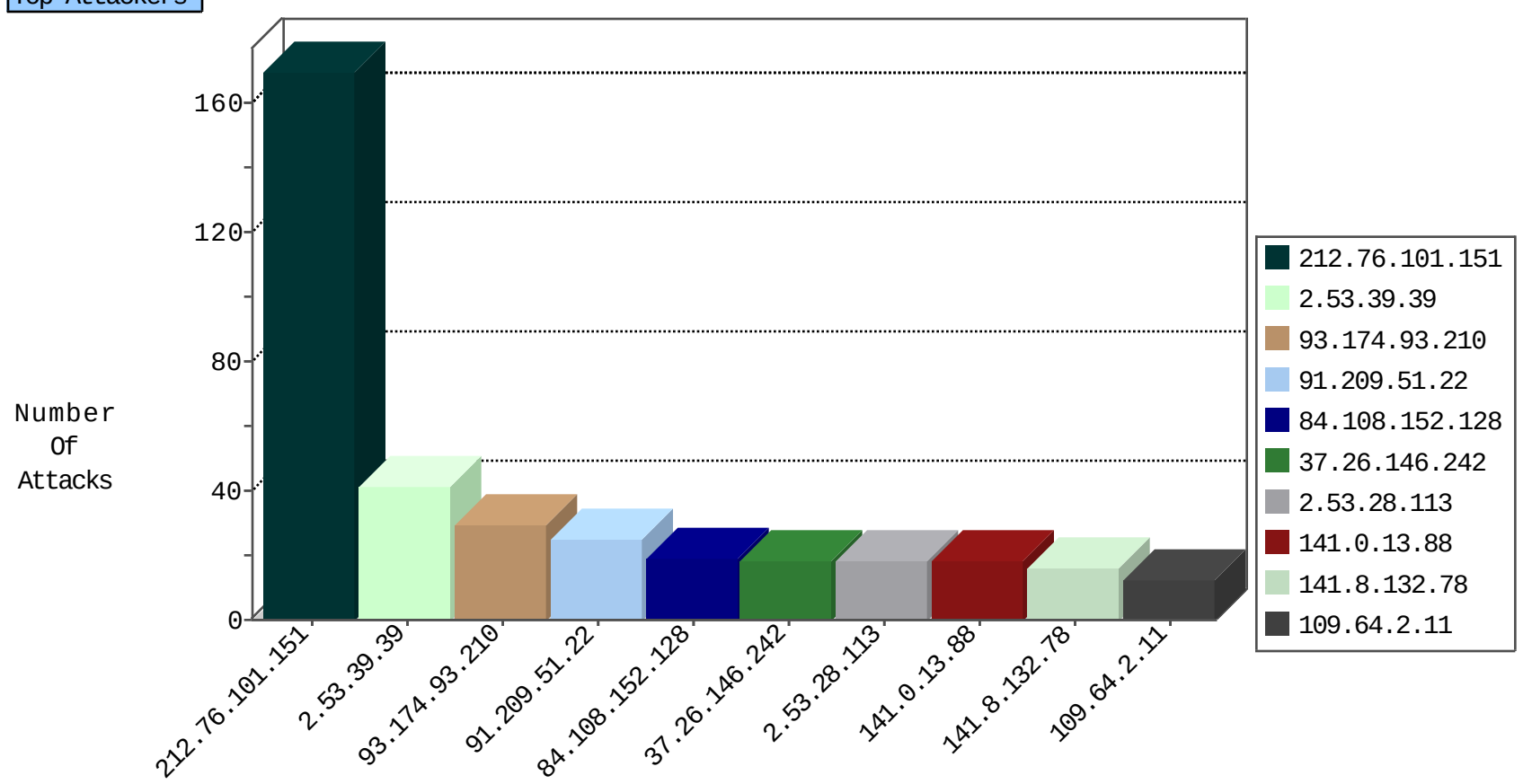
10-04-2016-23:04:02 to 10-05-2016-00:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-04-2016-23:04:02 to 10-05-2016-00:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.249.181.44	Sweden	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	19
95.86.100.91	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
93.174.93.210	Netherlands	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
93.174.93.210	Netherlands	147.237.72.166	aka.idf.il	block-sp-traf1	forward	2
93.174.93.210	Netherlands	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
71.6.216.61	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	1

10-04-2016-23:04:02 to 10-05-2016-00:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.209.51.22	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	22
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	1090: HTTP: IIS .asp Source Code Read	Permit	8
91.209.51.22	Ukraine	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
51.254.129.90	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-04-2016-23:04:02 to 10-05-2016-00:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
115.220.0.234	147.237.76.202	China	e.halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
62.210.97.79	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
46.229.223.8	147.237.76.39	Russian Federation	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.53.146	147.237.0.15	France	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
14.152.59.11	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
114.112.83.142	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
78.108.178.14	147.237.8.27	Czech Republic	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.176	China	matpash.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
211.149.222.5	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
211.149.222.5	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
195.154.53.146	147.237.77.179	France	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
195.154.53.146	147.237.0.34	France	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
195.154.53.146	147.237.0.19	France	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
14.152.59.11	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
211.149.222.5	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
208.100.26.228	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
195.154.53.146	147.237.8.24	France	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.0.200	China	m4u.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
195.154.53.146	147.237.0.33	France	idf.il	ET SCAN Potential SSH Scan	1

10-04-2016-23:04:02 to 10-05-2016-00:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.39.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
141.0.13.88	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
2.53.28.113	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.108.152.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
109.64.2.11	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
176.13.12.110	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.176.129.137	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
45.59.183.79	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
37.26.146.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
213.57.150.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
109.64.90.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.177.43.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.148.166	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
83.249.181.44	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
83.130.85.135	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.117.195.229	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.146.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.134.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.10.214	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.54.193.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
93.174.93.210	Netherlands	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
2.53.18.206	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.105.30	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
185.27.106.109	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	3
95.86.100.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.22.134.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
93.174.93.210	Netherlands	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
2.53.169.149	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	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	2
80.246.138.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
199.30.24.223	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
173.252.90.240	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.26.146.242	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
185.27.107.81	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
87.69.134.14	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.26.146.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
87.69.134.14	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.4.116.197	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
5.22.134.95	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.182.82.206	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
93.174.93.210	Netherlands	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
207.46.13.167	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
77.138.179.55	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.85.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.201.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
212.143.142.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

10-04-2016-23:04:02 to 10-05-2016-00:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.76.101.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	170
2.53.39.39	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
84.108.152.128	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
178.137.149.141	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/haredim/general.aspx	Block	4
37.26.146.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.28.113	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.117.195.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.65.137	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	2
213.57.150.242	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
85.250.164.136	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.64.151	Israel	147.237.76.86	navy.idf.il	Parameter Type Violation catId in www.navy.idf.il/navy/articles.aspx	Block	1
213.151.46.241	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
176.13.20.39	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 66.102.9.2	Block	1
207.46.13.46	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefront/faq/5.stm.	Block	1
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1150-he/dover.aspx	Block	1
45.33.79.110	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteyerua/	Block	1
176.13.20.39	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
79.176.68.22	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	1
207.46.13.46	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/contactus/	Block	1
93.174.93.210	Netherlands	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.funimation.com/	Block	1
66.249.76.72	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/m/modiin/general.aspx	Block	1
46.19.86.115	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
176.98.73.65	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/haredim/general.aspx	Block	1
79.183.56.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/null	Block	1
66.249.64.36	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8906-he/refuah.aspx	Block	1
2.53.169.149	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.65.189.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
66.249.64.148	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/general.aspx	Block	1
2.53.174.1	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
148.251.179.145	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
77.125.75.51	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
46.117.195.229	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.27.105.92	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1

10-04-2016-23:04:02 to 10-05-2016-00:04:02