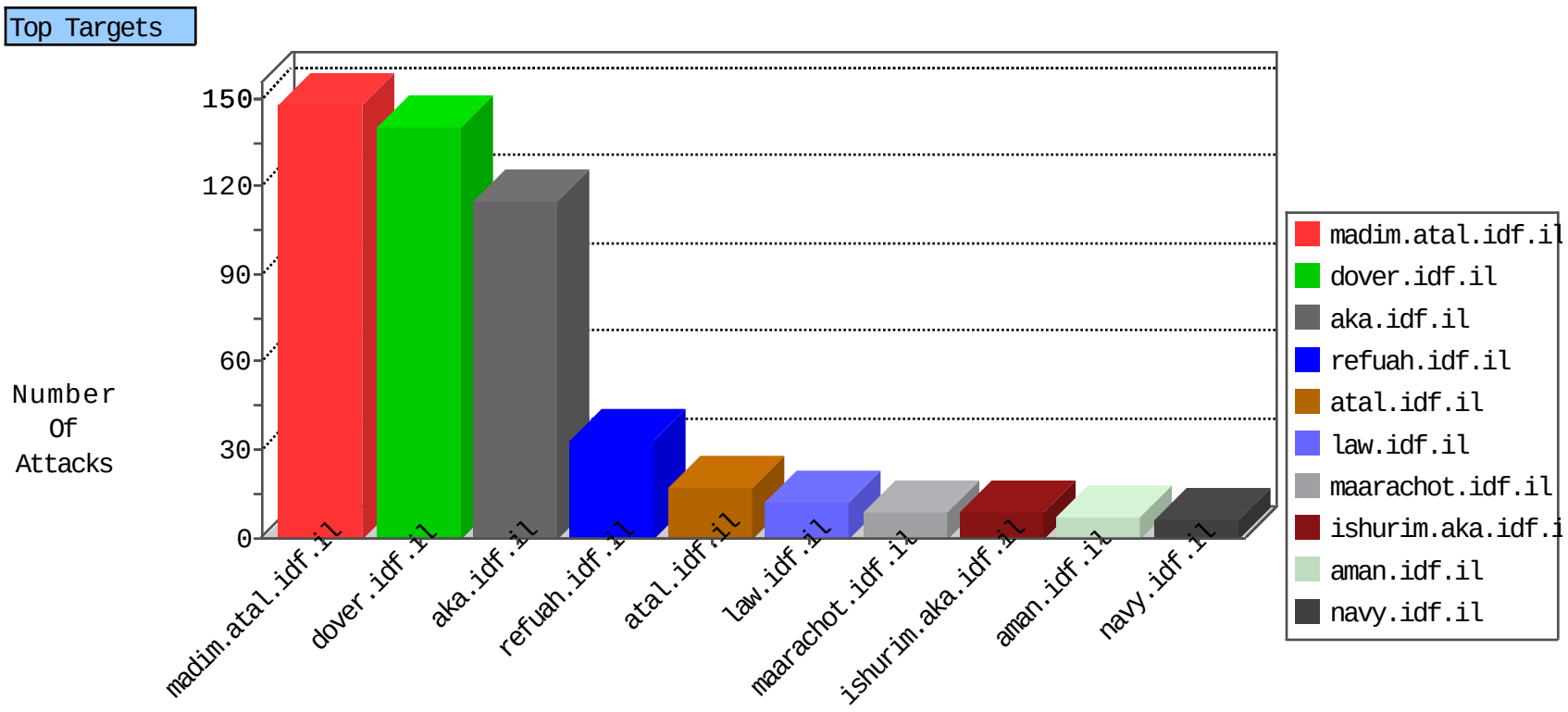
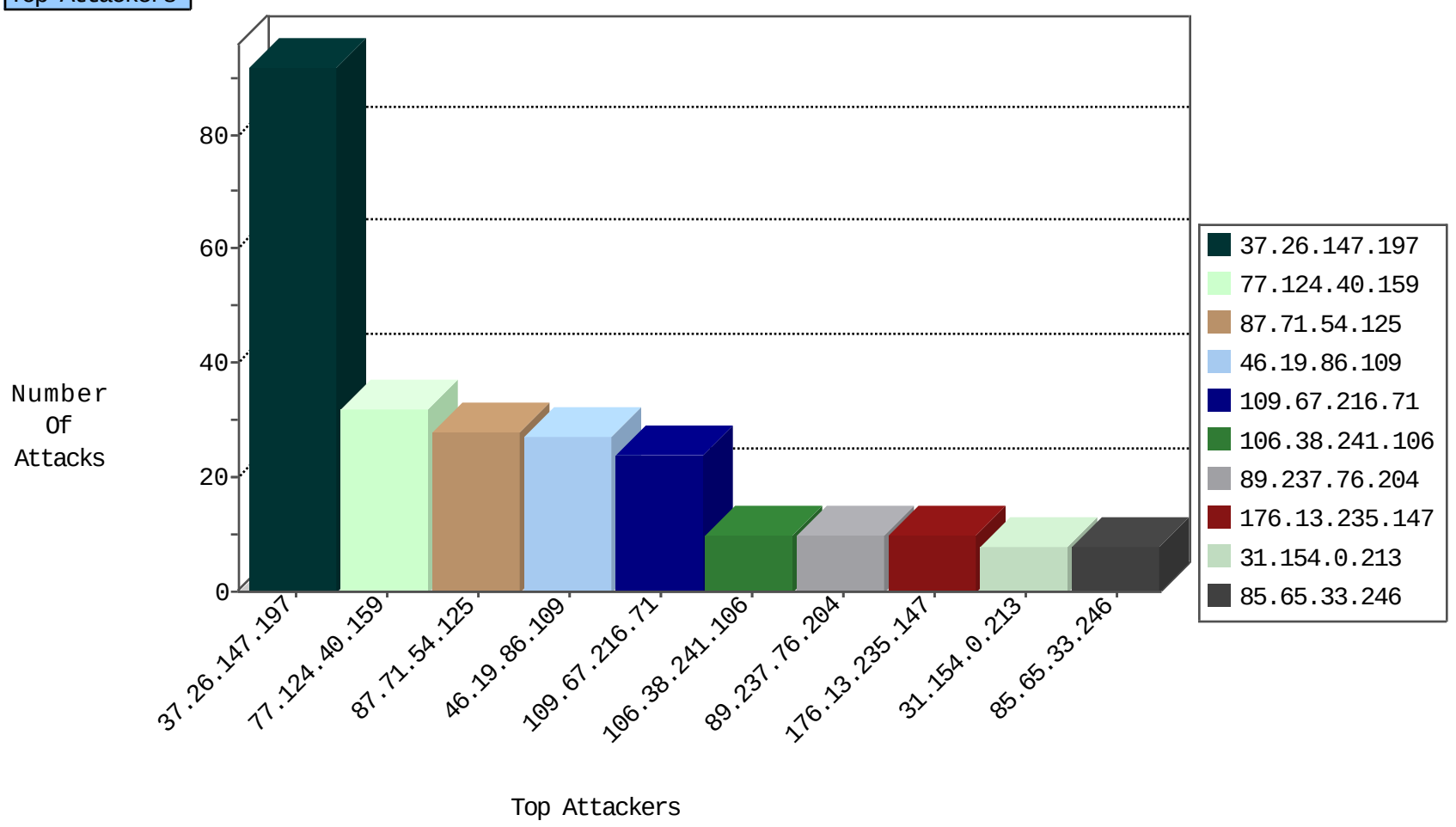
09-26-2016-20:04:09 to 09-26-2016-21:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-26-2016-20:04:09 to 09-26-2016-21:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.90.105	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	80
46.19.86.235	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
85.65.33.246	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
213.8.204.53	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
66.249.69.232	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
203.111.224.85	Philippines	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
80.178.251.210	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
84.110.54.112	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.86.75	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
194.177.16.3	Israel	147.237.76.86	navy.idf.il	Black List	drop	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
194.90.106.30	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-26-2016-20:04:09 to 09-26-2016-21:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	10
91.194.84.106	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3

09-26-2016-20:04:09 to 09-26-2016-21:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.163	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	3
37.26.147.197	147.237.0.19	Israel	madim.atal.idf.i	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
183.60.48.25	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
139.162.187.89	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
105.105.193.118	147.237.77.216	Algeria	dover.idf.il	portscan: TCP Distributed Portscan	1
84.238.218.60	147.237.77.212	Bulgaria	e.dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.142.6.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
178.207.88.218	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
139.162.13.205	147.237.77.179	Singapore	e.mazi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
95.163.144.203	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
78.129.171.173	147.237.76.176	United Kingdom	test.ncore.idf.i	ET SCAN Potential SSH Scan	1
46.183.223.228	147.237.0.34	Latvia	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
37.26.149.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-26-2016-20:04:09 to 09-26-2016-21:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.124.40.159	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
109.67.216.71	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
46.19.86.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
46.19.86.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.55.58.83	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.9.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.179.143.88	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.108.214.168	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
66.102.9.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.60	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.32.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.235.147	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
176.13.235.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
83.58.142.136	Spain	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
129.21.135.146	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.55.34.48	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
66.249.64.151	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.10.145	Israel	147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.86.255	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.235.147	Israel	147.237.72.166	aka.idf.il	SYN Attack		alert	2
185.120.125.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
46.19.86.43	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
66.102.9.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.181.10.145	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
5.22.134.96	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.23.165	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
109.253.158.33	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
85.65.33.246	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
109.66.34.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.85.127	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
207.244.70.169	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
24.37.167.35	Canada	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.177.33.33	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
87.69.67.205	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
209.58.129.109	United States	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
37.26.147.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
80.246.140.53	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.243.31.2	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.117.180.131	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.109.2.15	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
207.244.70.169	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
31.154.81.35	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.226.217.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
93.173.171.133	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
209.58.129.109	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

09-26-2016-20:04:09 to 09-26-2016-21:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
87.71.54.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
89.237.76.204	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 89.237.76.204	Block	9
46.19.86.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.147.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
31.154.0.213	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	4
46.19.86.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.251.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.135.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.131.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.154.0.213	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 31.154.0.213	Block	3
184.161.181.53	Canada	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	3
87.69.231.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.242.101	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	2
2.53.20.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.104.17	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
2.53.162.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.154	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/1093-7963-he/מאיר שחaspx.מו	Block	1
80.246.133.249	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/163-7173-he/	Block	1
204.79.180.192	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
77.138.201.236	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
2.53.171.134	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.67.216.71	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/71538.pdf	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
85.65.137.39	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
31.154.0.213	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/7/	Block	1
217.132.160.248	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
77.139.242.101	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.242.101	Block	1
68.180.228.99	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyuis	Block	1
89.237.76.204	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
66.249.66.233	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/894-he/nakhal.aspx)	Block	1
81.171.58.97	Netherlands	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
46.116.1.121	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
204.79.180.203	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx	Block	1
77.138.251.119	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
109.67.229.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/syncid=7664fafc-3f57-d04a-b4e0-2bfe3bcd7cbe	Block	1
66.249.76.117	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/894-he	Block	1
66.249.64.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
178.154.189.201	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/647-2350-en/patzar.aspx.	Block	1
104.254.252.50	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/main/	Block	1
66.249.69.170	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
82.81.199.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.6.3	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/sachar	Block	1
5.29.96.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.8.204.62	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
77.139.54.181	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/faq.aspx	Block	1
109.252.75.124	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.120	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894- he/matpash.aspx	Block	1

09-26-2016-20:04:09 to 09-26-2016-21:04:09