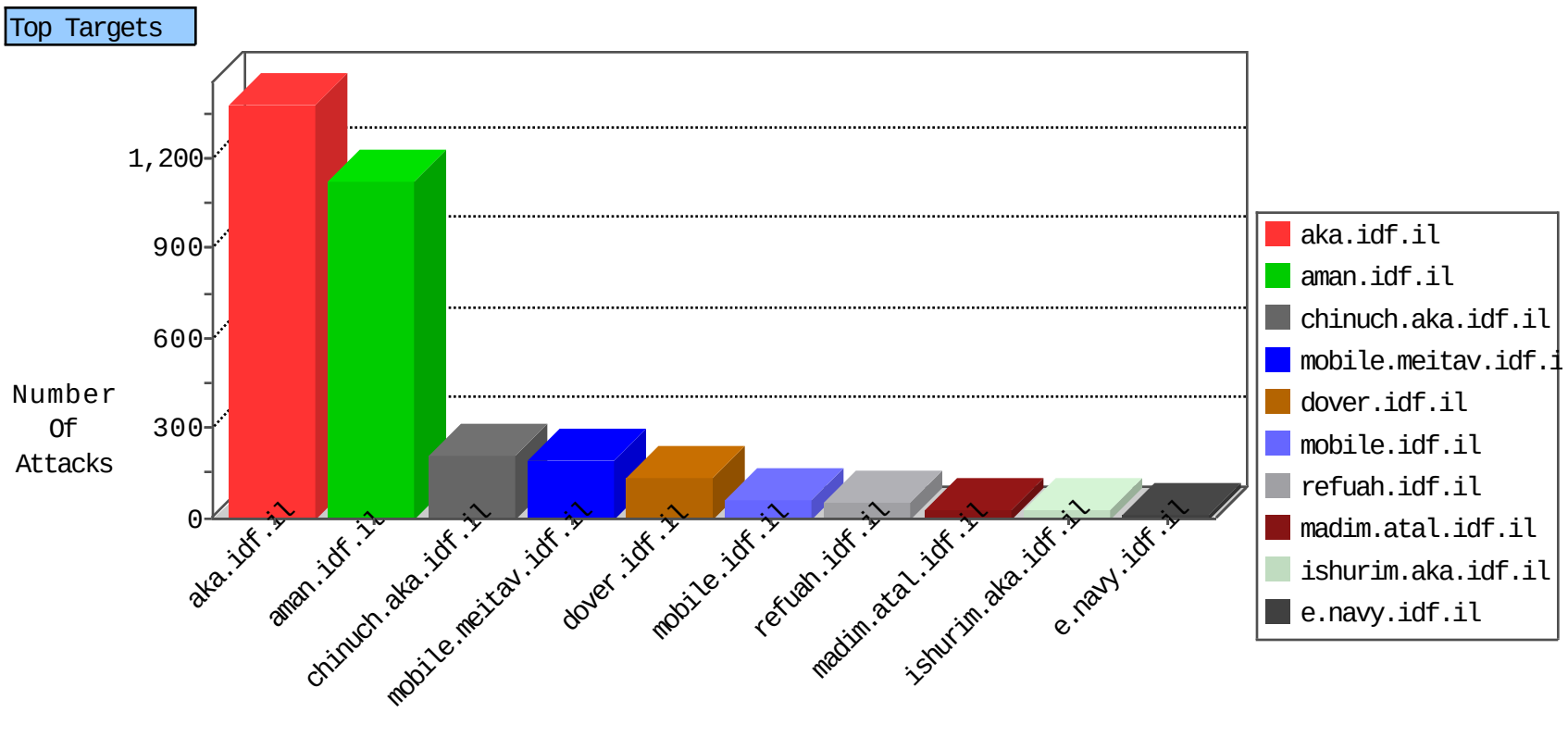
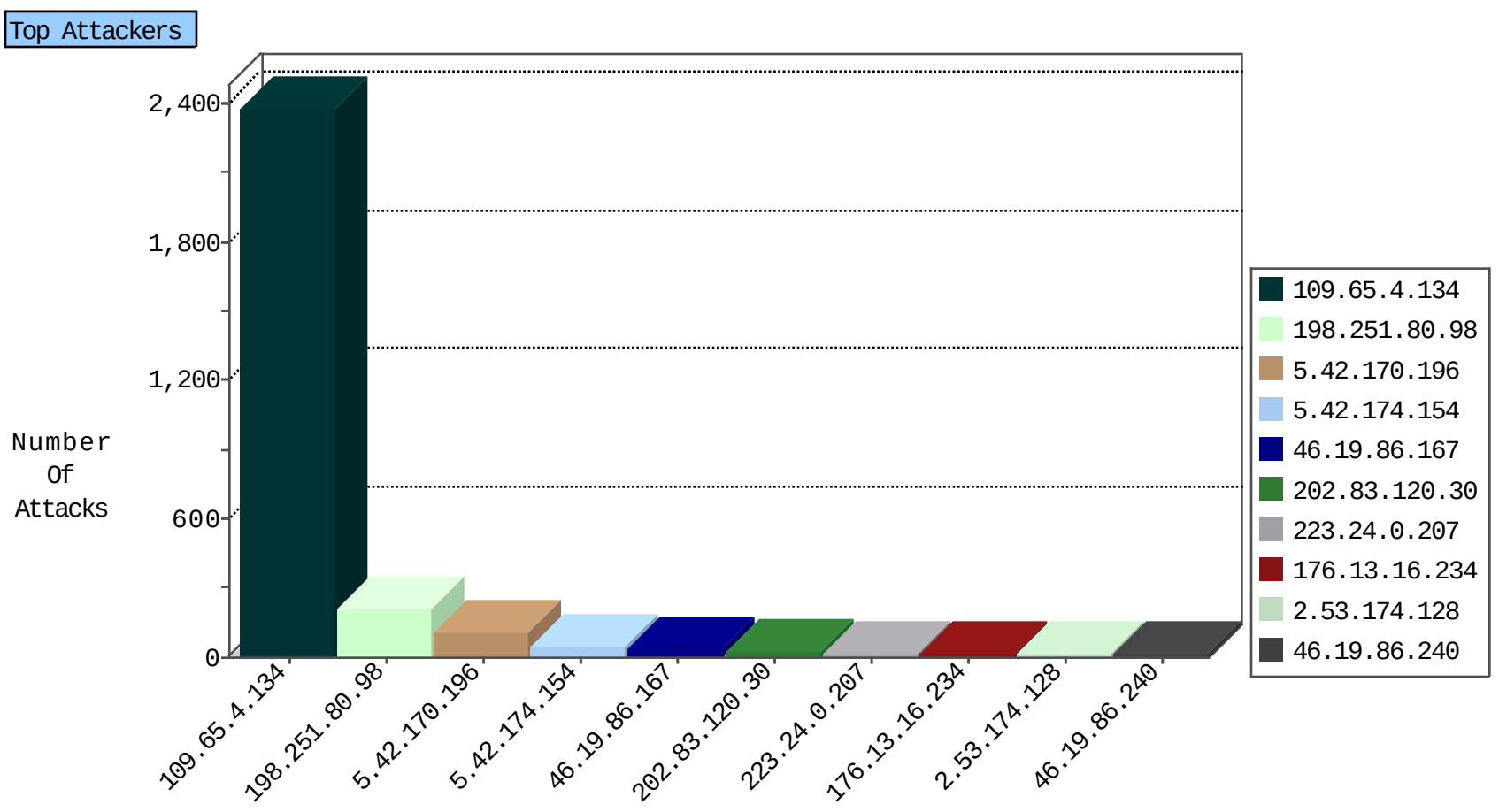
09-25-2016-23:04:00 to 09-26-2016-00:04:00

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-25-2016-23:04:00 to 09-26-2016-00:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.91.160.200	United States	147.237.8.46	e.chinuch.idf.il	Invalid TCP Flags	drop	1
180.97.106.37	China	147.237.76.202	e.halag.idf.il	Black List	drop	1
180.97.106.161	China	147.237.76.34	yohalan.idf.il	Black List	drop	1
180.97.106.162	China	147.237.76.197	e.himush.idf.il	Black List	drop	1

09-25-2016-23:04:00 to 09-26-2016-00:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.198.202	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-25-2016-23:04:00 to 09-26-2016-00:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
146.200.148.0	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
82.164.205.244	147.237.77.121	Norway	e.navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
117.191.73.198	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
109.75.46.199	147.237.0.35	Armenia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
105.156.8.191	147.237.77.179	Morocco	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.155	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.155	147.237.76.86	Ukraine	navy.idf.il	ET SCAN NMAP -sS window 1024	1
72.27.202.48	147.237.76.38	Jamaica	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
65.98.59.26	147.237.72.217	United States	e.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
117.191.73.198	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.75.35.87	147.237.77.243	Armenia	mobile.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
105.156.8.191	147.237.77.179	Morocco	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.155	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
72.27.202.48	147.237.76.38	Jamaica	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
58.218.200.137	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
191.96.249.189	147.237.0.34	Chile	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

09-25-2016-23:04:00 to 09-26-2016-00:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.65.4.134	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	75
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	26
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	26
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	24
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	22
223.24.0.207	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	16
46.19.86.167	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.167	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
5.42.170.196	France	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	13
5.42.170.196	France	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
5.42.170.196	France	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
5.42.170.196	France	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	12
5.42.170.196	France	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	12
5.42.170.196	France	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	12
5.42.170.196	France	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	12
5.10.231.162	Iraq	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	12
46.19.86.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
185.32.179.78	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.42.170.196	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.65.4.134	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
5.42.170.196	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
77.124.0.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.42.170.196	France	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
46.19.86.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.10.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.132.27.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.42.174.154	France	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.0.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
5.42.174.154	France	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
176.13.16.234	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
5.42.174.154	France	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.42.174.154	France	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
5.42.174.154	France	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
5.42.174.154	France	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
46.19.86.137	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.42.174.154	France	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
109.65.4.134	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5

09-25-2016-23:04:00 to 09-26-2016-00:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.4.134	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.65.4.134	Block	1147
109.65.4.134	Israel	147.237.72.156	aman.idf.il	Automated Vulnerability Scanning V1	Block	954
109.65.4.134	Israel	147.237.72.156	aman.idf.il	Multiple NULL Character in Parameter Value from 109.65.4.134	Block	124
109.65.4.134	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Parameter Value from 109.65.4.134	Block	45
2.53.174.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
109.65.4.134	Israel	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 109.65.4.134	Block	9
93.172.145.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	4
77.138.228.74	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	3
109.253.193.224	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	3
31.168.215.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
185.32.179.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.163.119	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	2
79.183.51.158	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.183.51.158	Block	2
77.249.247.187	Netherlands	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
31.154.81.16	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	2
2.53.140.104	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunderugshikulim.aspx	Block	2
109.65.4.134	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
31.154.81.16	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	2
66.249.64.169	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1677	Block	1
84.109.97.2	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
79.179.60.64	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
109.65.4.134	Israel	147.237.72.166	aka.idf.il	URL is Above Root Directory www.aka.idf.il/main/giyus/domainfiles/*//../../../../../../../../../../etc/passwd	Block	1
93.173.223.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.108.87.238	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed PHP Attempt	Block	1
2.55.60.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/size100x0/3365.jpg	Block	1
84.109.241.2	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
79.179.155.193	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
109.65.4.134	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login/	Block	1
64.251.27.99	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to /robots.txt	Block	1
84.108.87.238	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/wp-login.php	Block	1
193.190.253.150	Belgium	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	1
109.65.4.134	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.65.4.134	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.228	Block	1
5.22.134.110	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
84.111.206.216	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.114	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/apple-app-site-association	Block	1
109.65.4.134	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Parameter Encoding from 109.65.4.134	None	1
66.102.9.30	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
84.108.87.238	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
207.46.13.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19021-he/dover.aspx'½¿|'½¿|'•'½¿|'£	Block	1
66.249.73.186	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/iturim/asp/displayallsoldiers.asp	Block	1
80.82.24.129	Poland	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.138.167.190	France	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus	Block	1
157.55.39.135	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
66.249.64.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/assetlinks.json	Block	1
84.108.87.238	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
212.76.108.72	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1

09-25-2016-23:04:00 to 09-26-2016-00:04:00