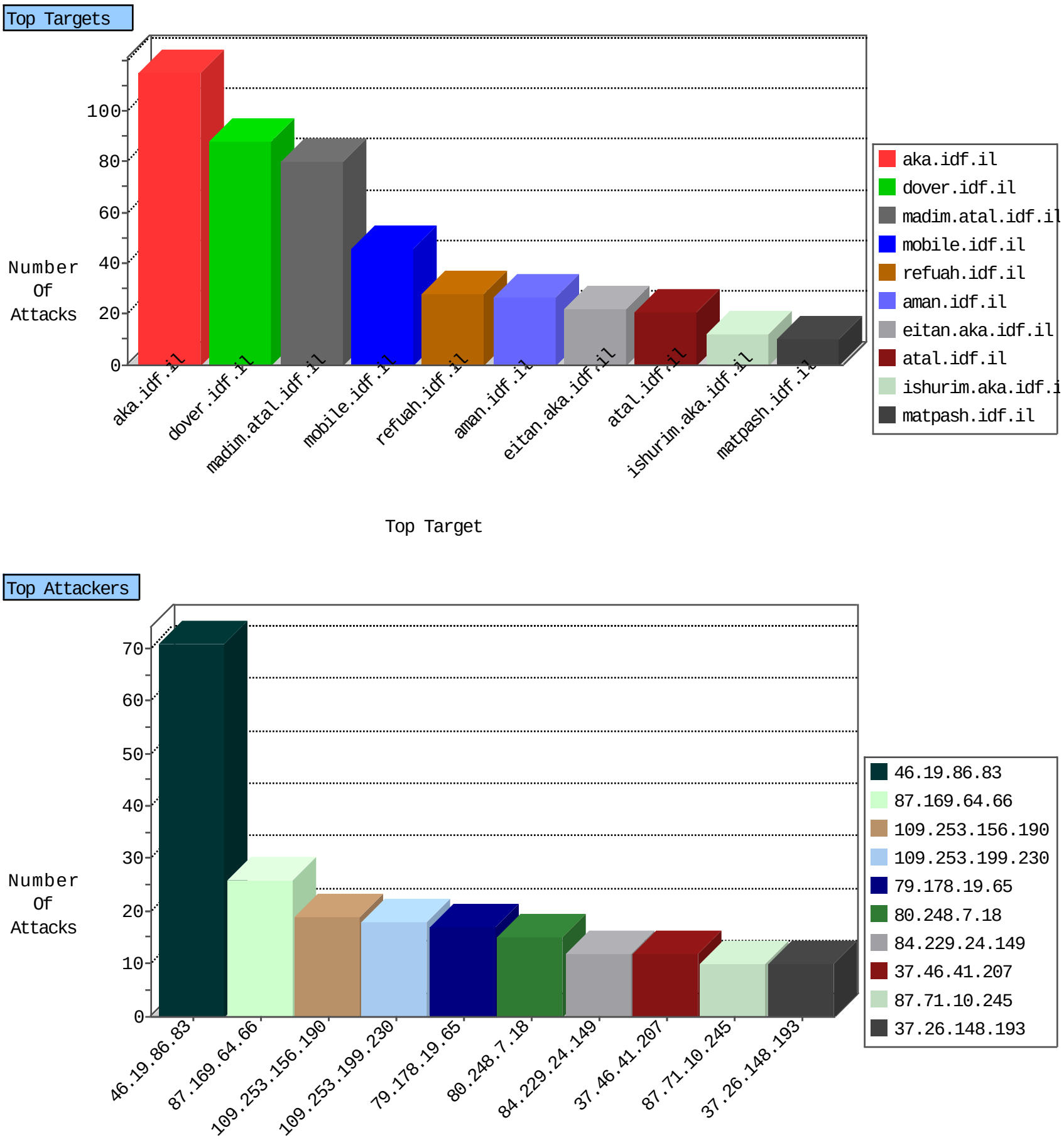
10-01-2016-11:04:01 to 10-01-2016-12:04:01

IDF Under Attack Daily Report



10-01-2016-11:04:01 to 10-01-2016-12:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
71.6.158.166	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
85.255.7.155	Poland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

10-01-2016-11:04:01 to 10-01-2016-12:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
5.9.62.130	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-01-2016-11:04:01 to 10-01-2016-12:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.248.7.18	147.237.0.35	Nigeria	akaws.idf.il	ET SCAN Potential SSH Scan	2
80.248.7.18	147.237.0.16	Nigeria	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
77.127.51.23	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
80.248.7.18	147.237.77.235	Nigeria	sviva.idf.il	ET SCAN Potential SSH Scan	2
80.248.7.18	147.237.72.217	Nigeria	e.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
58.220.2.5	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
125.78.68.61	147.237.76.44	China	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.220.2.5	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
80.248.7.18	147.237.77.243	Nigeria	mobile.idf.il	ET SCAN Potential SSH Scan	1
40.84.189.118	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
80.248.7.18	147.237.77.234	Nigeria	halag.idf.il	ET SCAN Potential SSH Scan	1
14.152.59.11	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
80.248.7.18	147.237.77.74	Nigeria	law.idf.il	ET SCAN Potential SSH Scan	1
80.248.7.18	147.237.76.30	Nigeria	himush.idf.il	ET SCAN Potential SSH Scan	1
80.248.7.18	147.237.72.166	Nigeria	aka.idf.il	ET SCAN Potential SSH Scan	1
80.248.7.18	147.237.0.34	Nigeria	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
194.224.101.170	147.237.76.86	Spain	navy.idf.il	ET SCAN NMAP -sS window 1024	1
58.220.2.5	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
104.214.108.211	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
40.121.139.43	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
40.68.159.134	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
80.248.7.18	147.237.77.233	Nigeria	atal.idf.il	ET SCAN Potential SSH Scan	1
80.248.7.18	147.237.76.38	Nigeria	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1

10-01-2016-11:04:01 to 10-01-2016-12:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.169.64.66	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
109.253.156.190	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
109.253.199.230	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
79.178.19.65	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
84.229.24.149	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.46.41.207	Israel	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	12
87.71.10.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.239	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
103.245.240.222	Bhutan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
202.91.66.102	India	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.66	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.201.154.142	Netherlands	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
207.46.13.107	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.212	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.65.27.109	Palestinian Territory Occupied	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
185.120.124.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
109.253.145.102	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
31.210.187.112	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.148.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
157.55.39.145	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.110.108.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
80.246.137.184	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
66.249.65.10	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.124.13	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
77.126.22.145	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.219.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
185.3.147.173	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.126.22.145	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
122.177.194.226	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
213.175.183.170	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
31.168.75.177	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
185.120.125.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	2
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
37.26.148.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
172.59.160.230	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
213.175.183.170	Lebanon	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.48	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
122.177.194.226	India	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
176.13.226.82	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
213.175.183.170	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.230	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
37.26.148.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
46.19.86.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
93.80.145.234	Russian Federation	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	71
109.253.192.3	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	6
31.210.187.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
147.236.69.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.57.157.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
82.166.121.189	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	2
83.178.235.218	Sweden	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	2
2.55.2.206	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/images/1.he/infocenteritem/	Block	2
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
2.55.56.33	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
66.249.65.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8802-he/refuah.aspx	Block	1
180.76.15.146	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
46.19.85.116	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method 2.1475311862.; in URL _pk_ses.118.fd1c=*	Block	1
87.71.10.245	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.139.28.69	France	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
66.249.65.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 79.181.99.166 (Open Mode)	None	1
68.180.228.238	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
180.76.15.150	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
93.157.83.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mains/sachar	Block	1
77.139.181.144	France	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	1
37.142.219.89	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/registrationwizard/register.aspx parameter	None	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
213.8.204.71	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
46.116.32.164	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.116.32.164	Block	1
2.53.51.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.172.97.67	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.176.112.142	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.176.112.142	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Method	Block	1
46.19.85.116	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version	Block	1
77.127.55.180	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/sachar	Block	1
46.116.32.164	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/_vti_bin/owssvr.dll	Block	1
213.8.204.71	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	1
109.64.136.10	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
79.176.112.142	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	1
180.76.15.144	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
46.19.85.116	Israel	147.237.76.42	refuah.idf.il	Malformed URL _pk_ses.118.fd1c=*	Block	1
85.64.211.139	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
77.138.87.96	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
109.66.124.214	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.178.19.65	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1