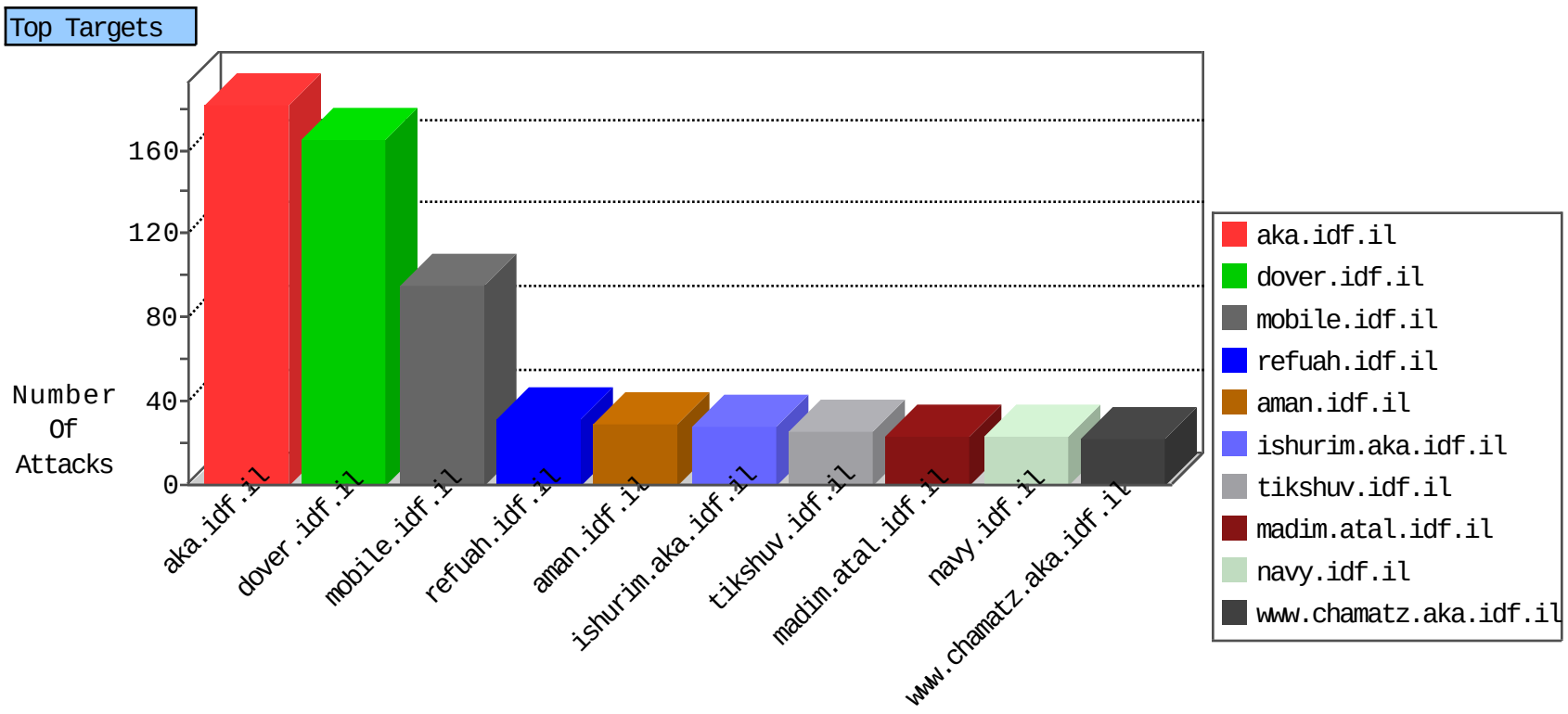
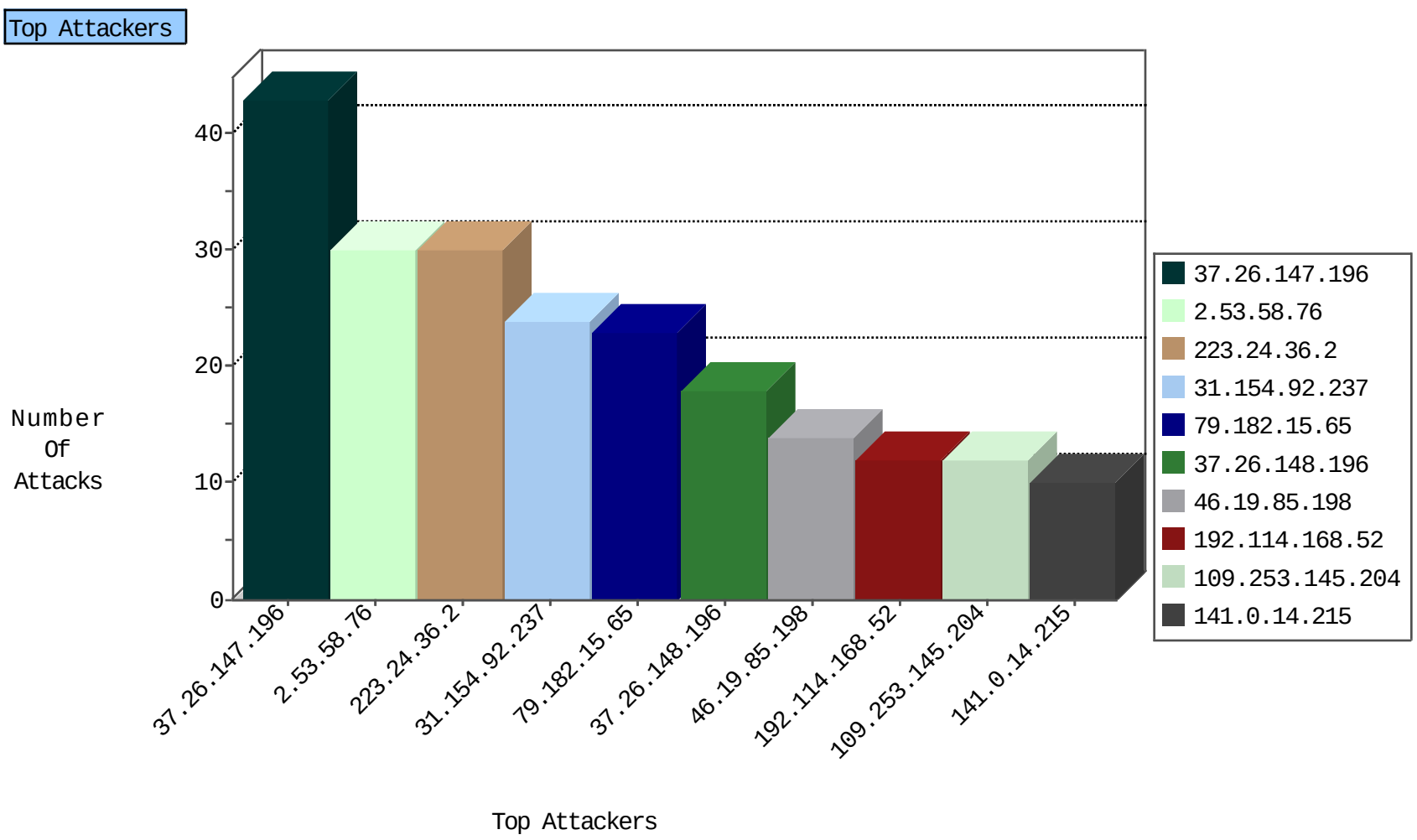
09-26-2016-17:04:02 to 09-26-2016-18:04:02

IDF Under Attack Daily Report





09-26-2016-17:04:02 to 09-26-2016-18:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.222.62	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
209.126.136.2	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
45.117.244.9	Fiji	147.237.0.34	tikshuv.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

09-26-2016-17:04:02 to 09-26-2016-18:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-26-2016-17:04:02 to 09-26-2016-18:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
27.97.139.181	147.237.76.200	India	eitan.aka.idf.il	GPL SCAN nmap TCP	4
188.120.154.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
110.142.17.64	147.237.0.16	Australia	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.87.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 3072	1
79.181.96.110	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sA (2)	1
46.116.200.19	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
40.114.15.49	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
212.235.31.125	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.106.139.19	147.237.77.74	Ireland	law.idf.il	ET SCAN NMAP -sS window 4096	1
2.98.56.16	147.237.0.33	United Kingdom	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.119.59.235	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.253.132.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.163.144.203	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
85.250.118.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.2.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.117.244.9	147.237.0.16	Fiji	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
213.151.38.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.38.68.132	147.237.72.14	Brazil	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
23.19.26.226	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1

09-26-2016-17:04:02 to 09-26-2016-18:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
223.24.36.2	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.53.58.76	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
31.154.92.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
109.253.145.204	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
141.0.14.215	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
37.26.147.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.147.196	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
37.26.147.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.114.168.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.182.15.65	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
80.246.139.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
80.246.138.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.86.130	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.32	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
176.13.2.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.15.65	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.114.7.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.196	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
192.116.55.97	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
77.127.39.211	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
37.26.147.196	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
80.246.140.123	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
37.26.148.196	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.147.196	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
2.53.21.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.147.196	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
79.181.28.218	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.198	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
80.246.136.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.198	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.87	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
77.127.39.211	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.135	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
141.0.15.222	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
212.199.95.73	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.29.237.38	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.76.0.101	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.101	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
217.132.55.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
37.26.148.196	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
176.12.160.5	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.17.210	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
37.26.149.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.94	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.15.65	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence		monitor	3
185.120.124.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
100.92.187.182		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2

09-26-2016-17:04:02 to 09-26-2016-18:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.46.37.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
62.159.95.94	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	5
109.253.141.5	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtLastName	Block	4
79.176.17.94	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
109.64.154.232	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
217.132.112.232	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.5.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.116.91	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	2
79.180.170.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.198	Israel	147.237.76.86	navy.idf.il	Distributed Malformed URL	Block	2
192.118.73.46	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	2
46.19.85.198	Israel	147.237.76.86	navy.idf.il	Distributed Unknown HTTP Request Method	Block	2
2.55.56.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.175.36	France	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.178.172.215	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	2
169.229.3.91	United States	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
67.53.18.178	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.198	Israel	147.237.76.86	navy.idf.il	Illegal HTTP Version _pk_ref.27.434e=%5B%22%22%2C%22%22%2C1474899725%2C%22https%3A%2F%2Fwww.google.co.il%2F%22%5D; _pk_id.27.434e=6e0b1db255ebe0b2.1474899725.1.1474899725.1474899725.; _pk_ses.27.434e=*	Block	1
80.179.9.115	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	1
2.55.148.254	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.200.77	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
176.13.233.183	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
113.103.82.244	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
66.102.6.3	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	1
87.69.211.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.76.124.226	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.178.251.128	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1361-he/dover.aspx	Block	1
46.19.86.178	Israel	147.237.76.42	refuah.idf.il	Distributed Illegal HTTP Version	Block	1
109.65.14.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.179.9.115	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/7/	Block	1
37.26.146.231	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
217.194.206.217	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kesher	Block	1
176.195.157.165	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunsummary.aspx	Block	1
113.103.82.244	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.102.9.8	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
89.139.182.120	Israel	147.237.76.42	refuah.idf.il	Illegal Parameter Encoding ctl00$ContentPlaceHolder1$ddlSubjectTextHidden in www.refua.atal.idf.il/1518-he/refuah.aspx	None	1
46.19.85.198	Israel	147.237.76.86	navy.idf.il	Abnormally Long Request request version	Block	1
212.117.153.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/selectusertype.asp	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
46.19.86.178	Israel	147.237.76.42	refuah.idf.il	Distributed Malformed URL	Block	1
109.67.136.38	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
80.246.136.197	Israel	147.237.77.243	mobile.idf.il	Multiple Untraceable SSL Sessions from 80.246.136.197 (Unknown SSL Session)	None	1
37.26.149.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.154.129	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunderugtafkidim.aspx	Block	1
180.76.15.13	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9014-he/refuah.aspx	Block	1

09-26-2016-17:04:02 to 09-26-2016-18:04:02