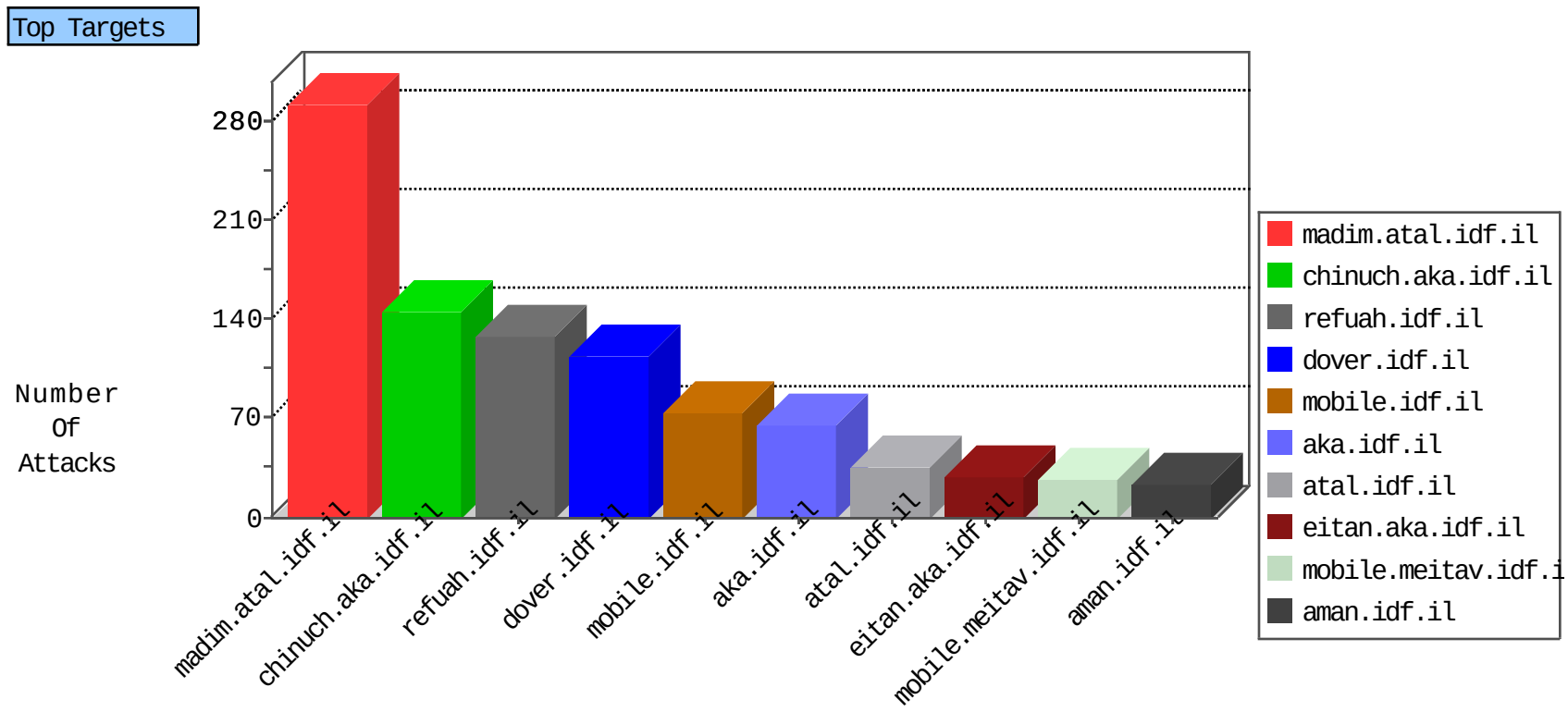
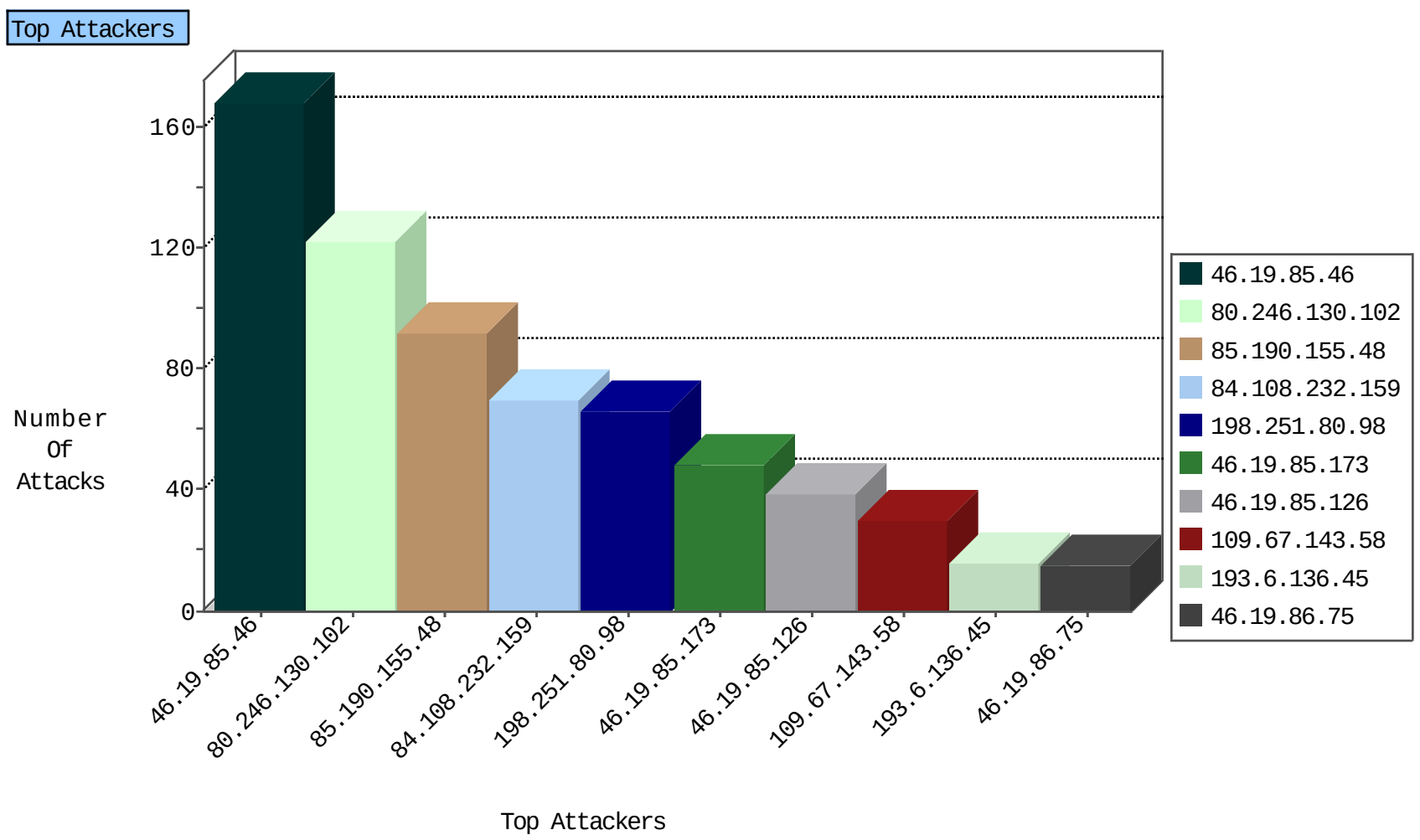
09-24-2016-23:04:01 to 09-25-2016-00:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-24-2016-23:04:01 to 09-25-2016-00:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.94.111.1	Russian Federation	147.237.76.201	e.atal.idf.il	Black List	drop	1

09-24-2016-23:04:01 to 09-25-2016-00:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
142.54.184.90	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
49.73.132.31	China	147.237.72.156	aman.idf.il	2226: Backdoor: TCP Window Size 55808 Trojan	Block	1

09-24-2016-23:04:01 to 09-25-2016-00:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.112.38.190	147.237.0.19	China	madim.atal.idf.il	GPL SCAN nmap TCP	2
116.77.72.71	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
103.56.164.194	147.237.8.27	Vietnam	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
218.103.242.29	147.237.77.234	Hong Kong	halag.idf.il	ET SCAN Potential SSH Scan	1
80.246.130.187	147.237.77.226	Israel	www.chamatz.aka.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
218.103.242.29	147.237.77.226	Hong Kong	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
61.147.247.161	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.103.242.29	147.237.77.212	Hong Kong	e.dover.idf.il	ET SCAN Potential SSH Scan	1
37.26.147.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.103.242.29	147.237.77.170	Hong Kong	maarachot.idf.il	ET SCAN Potential SSH Scan	1
192.223.72.100	147.237.76.86	Bolivia	navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
125.64.94.206	147.237.77.216	China	dover.idf.il	GPL WEB_SERVER WEB-MISC JBoss web-console access	1
116.77.72.71	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
103.56.164.194	147.237.8.27	Vietnam	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
103.56.164.194	147.237.8.27	Vietnam	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
218.103.242.29	147.237.77.227	Hong Kong	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
66.102.9.157	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
218.103.242.29	147.237.77.216	Hong Kong	dover.idf.il	ET SCAN Potential SSH Scan	1
41.215.36.46	147.237.76.34	Kenya	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
218.103.242.29	147.237.77.179	Hong Kong	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
177.43.168.115	147.237.76.200	Brazil	eitan.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
116.77.72.71	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1

09-24-2016-23:04:01 to 09-25-2016-00:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
80.246.130.102	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	121
109.67.143.58	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
85.190.155.48	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	17
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
85.190.155.48	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
85.190.155.48	Germany	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	16
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	16
193.6.136.45	Hungary	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
85.190.155.48	Germany	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	15
46.19.85.173	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.19.85.173	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	14
79.180.19.205	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.85.163	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
46.19.86.75	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.190.155.48	Germany	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.86.42	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
85.64.39.237	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.231.197.13	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.85.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.35.69	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.226.218.33	Israel	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
2.53.168.50	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
173.73.207.159	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
85.190.155.48	Germany	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
87.69.244.43	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.190.155.48	Germany	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
66.102.9.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.66.129.137	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	3
87.70.37.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
85.190.155.48	Germany	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	3
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.194.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
85.190.155.48	Germany	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
46.19.86.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.179.194.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.163	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.53.169.234	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
212.179.194.192	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.118	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.146.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.117.194.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.146.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	2
185.32.179.211	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	168
84.108.232.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
46.19.85.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
84.109.235.191	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.109.235.191	Block	9
125.64.94.206	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 125.64.94.206	Block	4
46.19.85.118	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/milluim/index	Block	3
176.13.18.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.17.180	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	3
176.13.229.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.135.209	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	2
46.19.86.75	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.228.34.6	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	2
37.26.146.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.35.69	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
66.249.66.131	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
92.222.85.77	France	147.237.77.176	matpash.idf.il	Unauthorized HTTP Method	Block	1
42.96.149.69	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.76.126	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/mobile/	Block	1
125.64.94.206	China	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
79.178.35.69	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.235	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/m/	Block	1
92.222.85.77	France	147.237.77.176	matpash.idf.il	Unauthorized Method OPTIONS for /	Block	1
77.138.76.247	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
46.120.239.118	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
84.109.235.191	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/giyus/login.aspx	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8746-he/refuah.aspx	Block	1
100.13.130.4	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/index.php	Block	1
84.108.232.159	Israel	147.237.0.19	madim.atal.idf.il	Multiple Untraceable SSL Sessions from 84.108.232.159 (Open Mode)	None	1
77.138.131.20	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.131.20	Block	1
46.121.145.214	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
125.64.94.206	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/test_404_page/	Block	1
85.64.24.221	Israel	147.237.72.166	aka.idf.il	Unknown Parameter asm in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
40.77.167.41	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
79.179.190.143	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2400.jpg	Block	1
103.244.14.50	Bangladesh	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
84.108.232.159	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.138.131.20	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	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
85.65.233.237	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
42.96.149.69	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
80.246.130.102	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2427.jpg	Block	1
109.64.135.201	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
84.109.118.53	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1

09-24-2016-23:04:01 to 09-25-2016-00:04:01