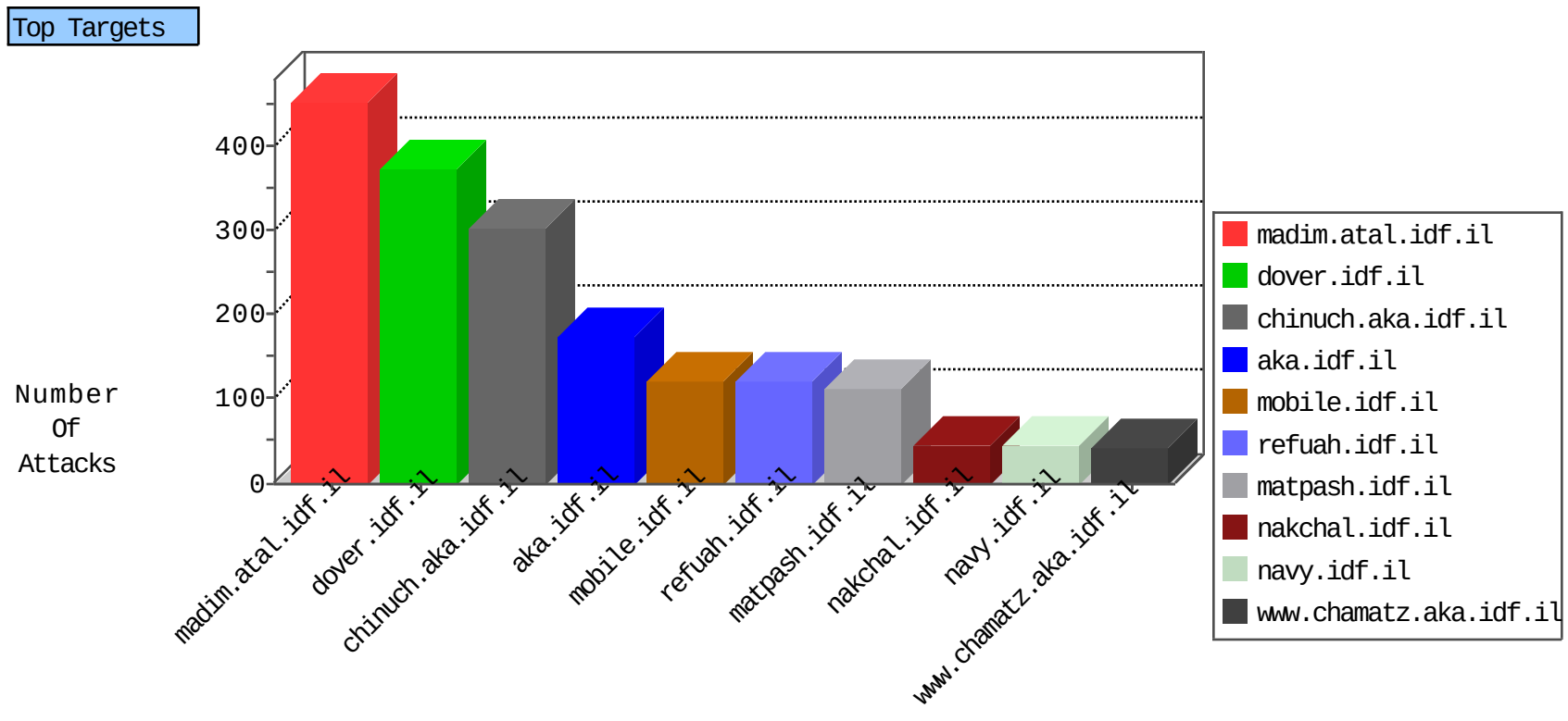
09-27-2016-16:04:02 to 09-27-2016-17:04:02

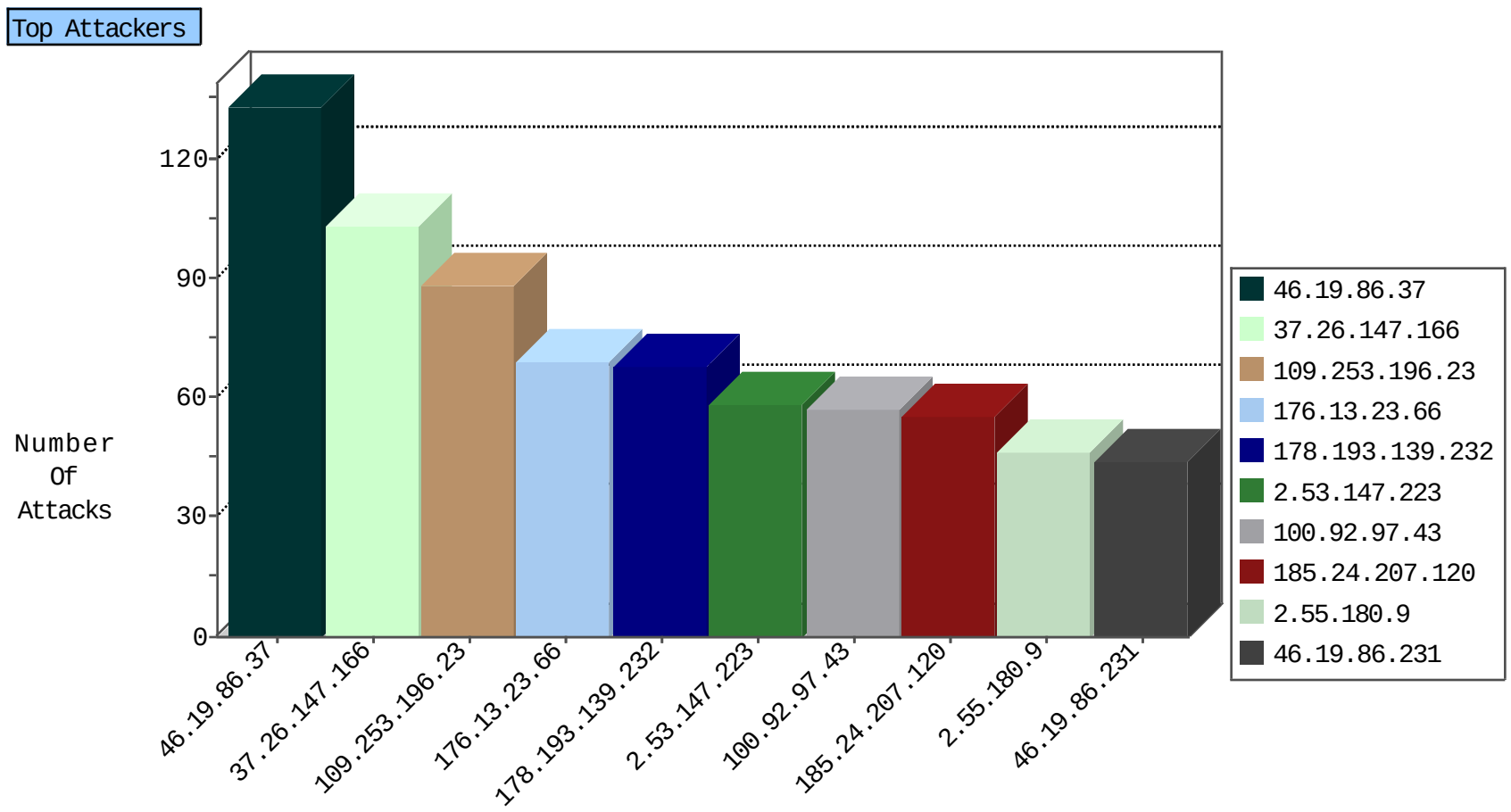
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-27-2016-16:04:02 to 09-27-2016-17:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
216.172.142.204	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	4006
98.207.0.127	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
66.249.69.228	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
185.94.111.1	Russian Federation	147.237.76.176	test.ncore.idf.il	Black List	drop	1
45.32.200.182	Netherlands	147.237.76.202	e.halag.idf.il	Black List	drop	1
207.232.37.85	Israel	147.237.77.216	dover.idf.il	HTTP-MISC-MS-Windows-HTTP-DOS	dest-reset	1

09-27-2016-16:04:02 to 09-27-2016-17:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.211.21	Israel	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	4
69.30.213.138	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.213.138	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	1

09-27-2016-16:04:02 to 09-27-2016-17:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.81.76.144	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
222.186.56.200	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.140.145	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.146.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.154.17.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.122.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.161.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.174.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.200	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.177.102.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.7.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.49.82.93	147.237.77.216	Kenya	dover.idf.il	portscan: TCP Distributed Portscan	1
77.139.79.85	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
77.126.85.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
141.0.14.224	147.237.72.166	Europe	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.1.0	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
103.207.37.82	147.237.77.234	Vietnam	halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.161.40.17	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
93.114.136.4	147.237.77.226	Romania	www.chamatz.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.19.85.83	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.139.141.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.166.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.9.176	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.55.17.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.55.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.36.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
78.129.171.173	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
211.149.222.5	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
77.139.67.95	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
149.255.108.192	147.237.8.46	United Kingdom	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
77.125.83.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.64.145.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-27-2016-16:04:02 to 09-27-2016-17:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
100.92.97.43		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	50
27.55.45.165	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
5.45.255.84	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
2.53.177.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
185.24.207.120	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
185.24.207.120	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
46.19.86.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
2.53.18.168	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.66.18.208	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	20
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	15
192.118.27.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
176.13.23.66	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
176.13.23.66	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
46.19.85.16	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.19.85.16	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	14
46.19.86.231	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.86.231	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	11
62.219.129.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
46.174.48.100	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	10
46.174.48.100	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.174.48.146	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.55.180.9	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	10
178.193.139.232	Switzerland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.253.147.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.174.48.146	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	9
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.174.48.100	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	9
2.55.180.9	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.174.48.146	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	9
46.19.86.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
109.64.24.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.86.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
176.13.23.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
2.55.180.9	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
109.64.24.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	8
2.53.150.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
2.55.180.9	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
46.174.48.146	Russian Federation	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
109.253.211.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.214.193	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
100.92.97.43		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.23.66	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
176.13.1.188	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.218	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.100	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.218	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

09-27-2016-16:04:02 to 09-27-2016-17:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	133
37.26.147.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	98
109.253.196.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	88
2.53.147.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
195.189.193.1	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 195.189.193.1	Block	25
46.19.86.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
37.26.147.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
109.253.140.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
109.253.212.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
81.218.34.242	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	5
195.199.204.102	Hungary	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	Block	5
37.26.147.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.253.212.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
74.216.182.82	Canada	147.237.77.176	matpash.idf.il	Distributed Unauthorized HTTP Method	Block	2
46.19.86.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.241.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.139.119.199	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	2
2.53.40.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
74.216.182.82	Canada	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
81.218.34.242	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
46.19.86.82	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
157.55.39.60	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/kamlar/klali/default.asp	None	1
5.29.106.116	Israel	147.237.72.166	aka.idf.il	Unauthorized Request Content Type text/ping	Block	1
77.138.196.0	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.157.54.26	Denmark	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	1
118.193.155.206	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
43.226.15.161	Cambodia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
82.81.76.144	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 82.81.76.144	Block	1
212.235.115.155	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.235.115.155	Block	1
109.253.144.80	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
217.194.195.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.189.193.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/s	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
118.193.155.206	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
46.19.85.100	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtPhone in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
2.53.18.168	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
82.81.76.144	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus	Block	1
74.216.182.82	Canada	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	1
212.235.115.155	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/3/	Block	1
50.117.45.145	United States	147.237.77.216	dover.idf.il	Unauthorized Method POST for 147.237.77.216/	Block	1
180.76.15.134	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9858-he/refuah.aspx	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9237-he/refuah.aspx	Block	1
129.85.51.22	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
95.86.90.65	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
213.8.129.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.0.67.97	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
185.56.72.220	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1

09-27-2016-16:04:02 to 09-27-2016-17:04:02