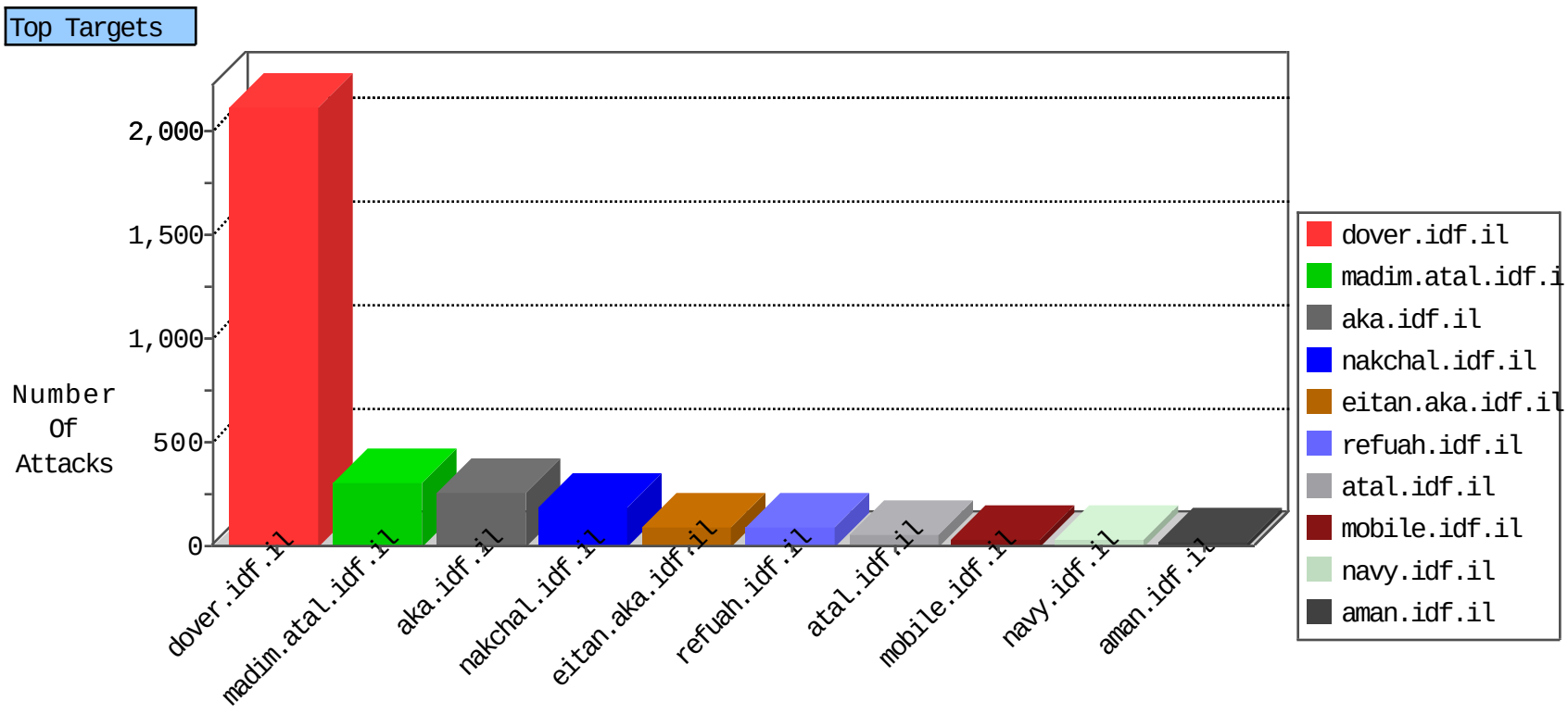
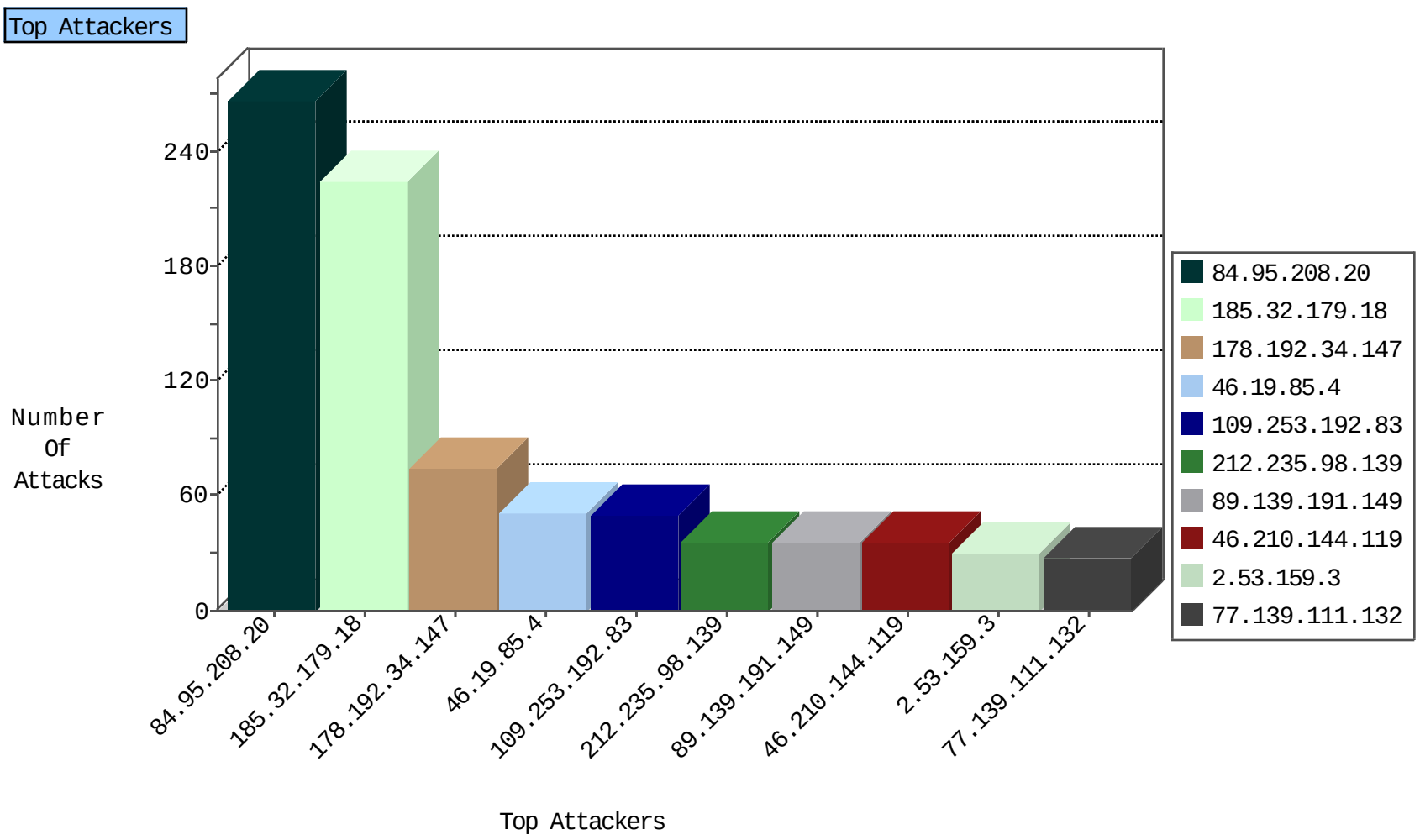
09-28-2016-12:04:02 to 09-28-2016-13:04:02

IDF Under Attack Daily Report





09-28-2016-12:04:02 to 09-28-2016-13:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.141.74	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
31.168.240.21	Israel	147.237.72.156	aman.idf.il	Black List	drop	2
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Black List	drop	1
188.138.102.157	Germany	147.237.76.42	refuah.idf.il	Black List	drop	1
79.177.196.109	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
188.138.102.157	Germany	147.237.76.44	e.refuah.idf.il	Black List	drop	1
91.230.121.156	Ukraine	147.237.76.200	eitan.aka.idf.i	Black List	drop	1
93.174.94.235	Netherlands	147.237.76.201	e.atal.idf.il	Black List	drop	1

09-28-2016-12:04:02 to 09-28-2016-13:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
240.0.10.13		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	2
37.26.148.247	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-28-2016-12:04:02 to 09-28-2016-13:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.86.254	147.237.76.31	Israel	nakchal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
84.108.30.238	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.178.204.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.161.124	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.253.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
202.155.58.28	147.237.76.199	Indonesia	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.55.141.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
125.65.82.44	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
80.246.137.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.104.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.57.53.85	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
46.121.79.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
202.155.58.28	147.237.76.196	Indonesia	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
179.43.141.198	147.237.77.212	Switzerland	e.dover.idf.il	ET SCAN Potential SSH Scan	1
109.65.167.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-28-2016-12:04:02 to 09-28-2016-13:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.139.191.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	36
2.53.159.3	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
77.139.111.132	France	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
82.166.195.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
62.0.200.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
62.0.206.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
46.19.85.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
212.143.144.153	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
176.13.241.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
46.210.144.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	16
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	16
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.86.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.253.194.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	14
46.19.85.99	Israel	147.237.76.31	nakchal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
62.0.251.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.116.54.47	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
93.172.148.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
62.0.252.97	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
84.94.199.17	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
193.43.244.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
87.70.46.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
152.62.109.204	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
62.219.162.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.253.207.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
213.6.126.27	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.4	Israel	147.237.76.31	nakchal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
82.81.222.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
185.120.126.3	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
2.53.1.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.137.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8

09-28-2016-12:04:02 to 09-28-2016-13:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	224
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	99
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	85
109.253.192.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	39
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	11
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	6
109.253.222.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
62.219.21.30	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	5
176.13.243.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
46.19.86.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.229.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.180	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.180	Block	3
37.26.147.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
212.179.224.187	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
132.72.86.150	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
212.205.110.227	Greece	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
81.218.251.252	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	2
77.138.176.236	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	2
66.249.66.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
81.218.251.252	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/	Block	1
62.219.21.30	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
46.19.85.145	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
195.212.29.180	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
80.255.185.2	Russian Federation	147.237.76.86	navy.idf.il	Malformed HTTP Header Line 3	Block	1
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
2.55.136.163	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.157	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	1
80.255.185.2	Russian Federation	147.237.76.86	navy.idf.il	NULL Character in Header Name at	Block	1
77.139.59.34	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	1
37.26.147.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
180.76.15.21	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/shared/clientscripts/jquery/' + url + '	Block	1
66.249.66.239	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
80.255.185.2	Russian Federation	147.237.76.86	navy.idf.il	Malformed URL	Block	1
74.91.23.166	United States	147.237.77.216	dover.idf.il	Unauthorized Method HEAD for 147.237.77.216/	Block	1
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
121.214.173.148	Australia	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.255.185.2	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/changelog.txt	Block	1
46.116.54.47	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
180.76.15.137	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9687-he/refuah.aspx	Block	1
77.139.111.132	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
2.53.149.127	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
85.140.5.104	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1

09-28-2016-12:04:02 to 09-28-2016-13:04:02