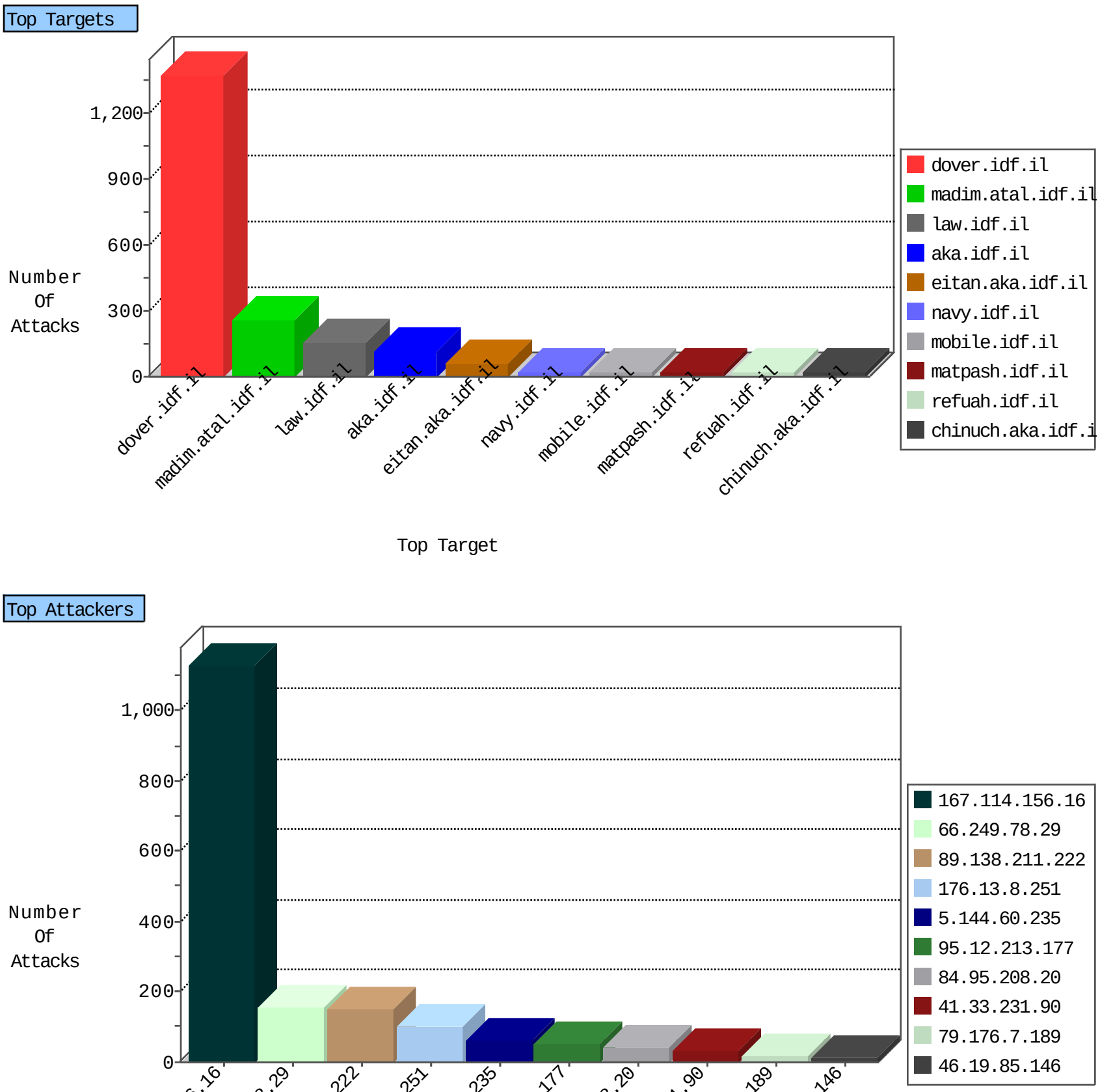
04-15-2016-14:04:05 to 04-15-2016-15:04:05

IDF Under Attack
Daily Report



04-15-2016-14:04:05 to 04-15-2016-15:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1132
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
109.67.206.55	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
14.189.238.126	Vietnam	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.2	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
204.42.253.2	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	2
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
14.182.204.228	Vietnam	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1

04-15-2016-14:04:05 to 04-15-2016-15:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.153.33	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.4.116.197	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
66.194.11.113	United States	147.237.77.176	matpash.idf.il	C1000008: HTTP: Xenu UserAgent	Block	2
95.12.213.177	Turkey	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	2
66.194.11.113	United States	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.106	France	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.249.66.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.162	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.194.11.113	United States	147.237.77.74	law.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
95.12.213.177	Turkey	147.237.76.147	chinuch.aka.idf.il	C1000016: HTTP: administrator in URI	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-15-2016-14:04:05 to 04-15-2016-15:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.29	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	155
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
91.201.236.158	147.237.76.197	Ukraine	e.himush.idf.il	ET SCAN NMAP -f -sS	1
87.229.116.42	147.237.76.38	Hungary	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
80.82.78.38	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.76.31	Latvia	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
185.103.252.14	147.237.76.148	Russian Federation	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
106.184.2.29	147.237.0.35	Japan	akaws.idf.il	ET SCAN Potential SSH Scan	1
95.12.213.177	147.237.76.147	Turkey	chinuch.aka.idf.il	SERVER-WEBAPP admin.php access	1
91.201.236.158	147.237.76.197	Ukraine	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
87.229.116.42	147.237.76.38	Hungary	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
87.229.116.42	147.237.8.14	Hungary	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
220.179.172.185	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
106.186.113.67	147.237.0.35	Japan	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
95.12.213.177	147.237.77.216	Turkey	dover.idf.il	SERVER-WEBAPP admin.php access	1
91.201.236.158	147.237.76.197	Ukraine	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1

04-15-2016-14:04:05 to 04-15-2016-15:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.144.60.235	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
105.159.152.157	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
77.127.67.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.109	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.162.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
94.230.86.209	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.117.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.144.60.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.103	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
31.210.186.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.88.185.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
5.102.242.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.146.191	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.130.133.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
64.231.205.119	Canada	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	5
84.95.60.162	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.130.133.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.251	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.121.211.156	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.183.202.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.7.189	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
46.19.86.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
31.210.187.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.1.172	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant		monitor	3
79.176.7.189	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.86.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.39.241	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.33	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.7.189	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
79.176.7.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.64.234.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.244.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.7.189	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
176.4.21.217	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.134.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.164.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.139.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.7.189	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.53.186.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.2.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-15-2016-14:04:05 to 04-15-2016-15:04:05

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
207.46.13.2	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

04-15-2016-14:04:05 to 04-15-2016-15:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.211.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	151
176.13.8.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
95.12.213.177	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.12.213.177	Block	11
95.12.213.177	Turkey	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	8
95.12.213.177	Turkey	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 95.12.213.177	Block	7
79.181.39.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
95.12.213.177	Turkey	147.237.76.147	chinuch.aka.idf.i	Multiple Unauthorized URL Access from 95.12.213.177	Block	5
95.12.213.177	Turkey	147.237.76.147	chinuch.aka.idf.i	PHP Attempt	Block	4
95.12.213.177	Turkey	147.237.76.147	chinuch.aka.idf.i	Multiple Admin Blocking from 95.12.213.177	Block	3
84.108.182.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1518-he/	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.146	Block	2
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 46.19.85.146	Block	2
84.108.182.120	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 84.108.182.120	Block	2
109.67.154.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.161.9.6	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.161.9.6	Block	2
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.146	Block	2
95.12.213.177	Turkey	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/wp-login.php	Block	1
79.180.164.141	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1507-	Block	1
95.12.213.177	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
207.46.13.189	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	1
95.12.213.177	Turkey	147.237.76.147	chinuch.aka.idf.i	Admin Blocking	Block	1
66.249.66.50	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list6.htm	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
99.196.29.4	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
95.12.213.177	Turkey	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
176.52.42.86	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/asp/'	Block	1
141.212.122.161	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method s=5710d75764311c5c000 in URL	Block	1
31.210.186.55	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
95.86.85.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
213.191.130.145	Croatia	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
109.65.186.128	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1517-he/atal.aspx	Block	1
186.151.254.242	Guatemala	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.204	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.120.222.165	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.187.56.76	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
95.189.19.159	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-en/cogat.aspx	Block	1
213.191.130.145	Croatia	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 46.19.85.146	Block	1
194.187.168.214	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17570-	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
40.77.167.25	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
95.189.19.159	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/1043-en/cogat.aspx	Block	1

04-15-2016-14:04:05 to 04-15-2016-15:04:05