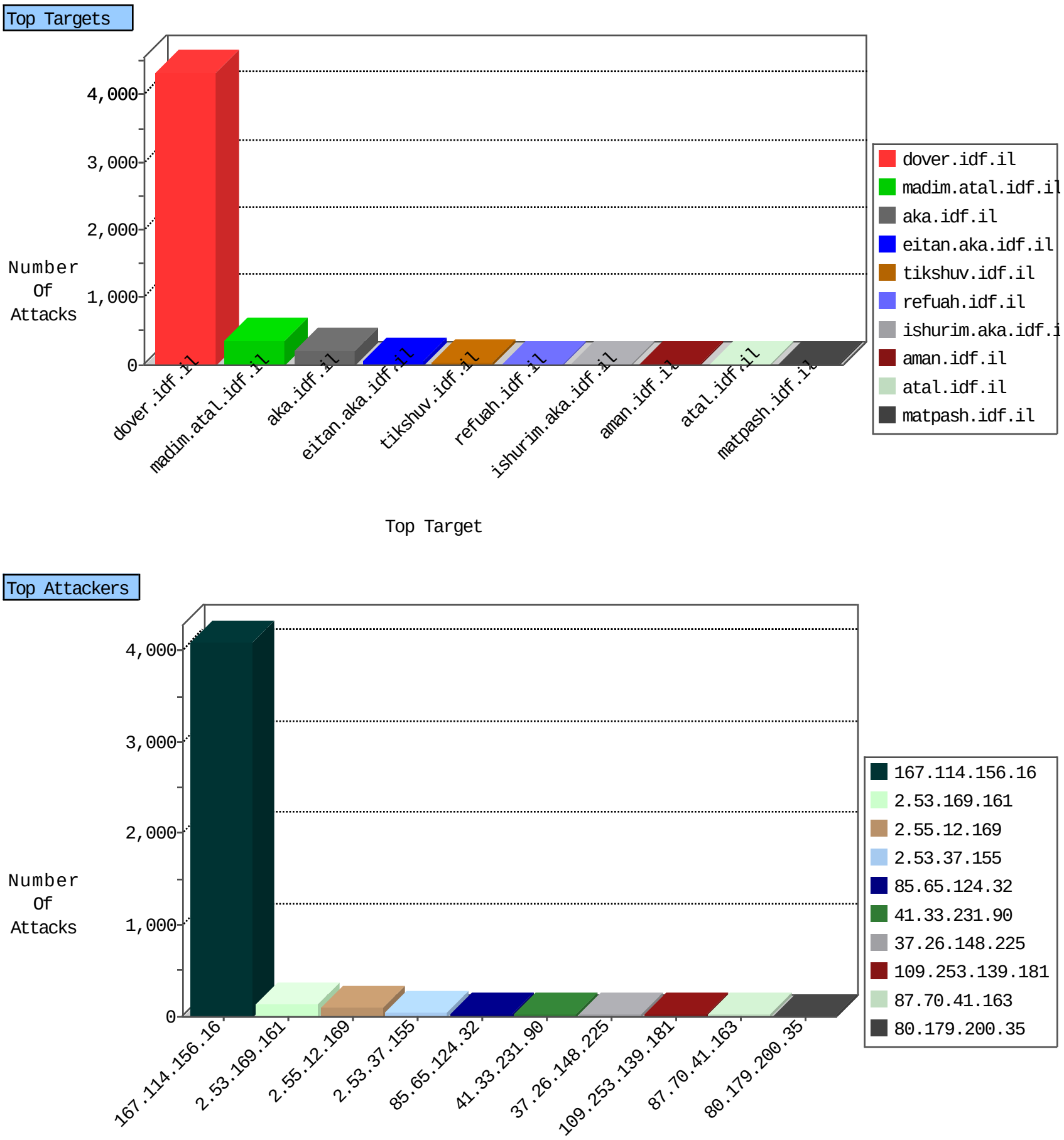
04-18-2016-10:04:03 to 04-18-2016-11:04:03

IDF Under Attack
Daily Report



04-18-2016-10:04:03 to 04-18-2016-11:04:03

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	4077
134.191.232.71	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	47
212.143.161.85	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
184.105.139.110	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.122	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.82	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.114	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
185.103.252.96	Russian Federation	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.106	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.118	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.74	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
194.90.119.123	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
184.105.139.110	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
91.205.155.82	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
184.105.139.118	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.74	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1

04-18-2016-10:04:03 to 04-18-2016-11:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
69.30.198.242	United States	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-18-2016-10:04:03 to 04-18-2016-11:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.19.85.143	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.194.205.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.114.146.227	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
149.50.73.148	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.219.238.10	147.237.76.38	United States	e.e.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
84.94.67.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.117.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.153.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.210.188.124	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
190.128.175.138	147.237.77.235	Paraguay	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
106.186.113.67	147.237.8.14	Japan	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
87.71.19.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
77.124.23.9	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

04-18-2016-10:04:03 to 04-18-2016-11:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
37.26.148.225	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
85.65.124.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
80.179.200.35	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
149.78.54.19	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.65.124.32	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.102.254.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.179.60.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.55.12.169	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
89.138.88.151	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
62.219.128.153	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
37.26.149.241	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.108.217.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.22.131.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.41.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
66.249.78.5	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.241	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.253.139.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.212.126	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.12.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.33.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.205	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.205	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.177.157.181	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
89.139.35.196	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.177.157.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
87.70.41.163	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
89.139.35.196	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.148.27.130	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.66.187	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.205.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.41.163	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
194.90.151.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.90.63.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.142.219.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
62.219.128.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.150.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.168.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.90.153.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-18-2016-10:04:03 to 04-18-2016-11:04:03

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.86.27	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3

04-18-2016-10:04:03 to 04-18-2016-11:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.169.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	143
2.55.12.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
2.53.37.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
109.253.139.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
212.143.173.198	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.143.173.198	Block	11
176.13.5.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
192.114.161.10	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/mobile	Block	8
2.55.178.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
31.168.144.189	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 31.168.144.189	Block	4
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.128.185	Block	4
2.53.182.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.18.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.5.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.114.161.10	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 192.114.161.10	Block	2
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
2.53.168.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
188.120.154.19	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	2
157.55.39.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
89.234.68.69	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.79.169	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
131.114.197.117	Italy	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
2.53.130.228	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/text.css	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
79.181.153.14	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
185.103.252.5	Russian Federation	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
46.19.85.205	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
157.55.39.202	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
89.234.68.81	Ireland	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
68.180.229.170	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
31.168.144.189	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	1
176.13.12.214	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
131.114.197.117	Italy	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
2.53.167.198	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
213.151.41.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.aspx/	Block	1
80.74.116.135	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
185.103.252.5	Russian Federation	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.64.234	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1238-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
212.143.173.198	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/back.png	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.146.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal/site/templates/controller.asp	Block	1
176.13.17.185	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	1
131.114.197.117	Italy	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
213.254.241.4	France	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$btnSearch in www.aka.idf.il/main/sachar/default.aspx	None	1
195.200.205.37	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
81.218.165.127	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1

04-18-2016-10:04:03 to 04-18-2016-11:04:03