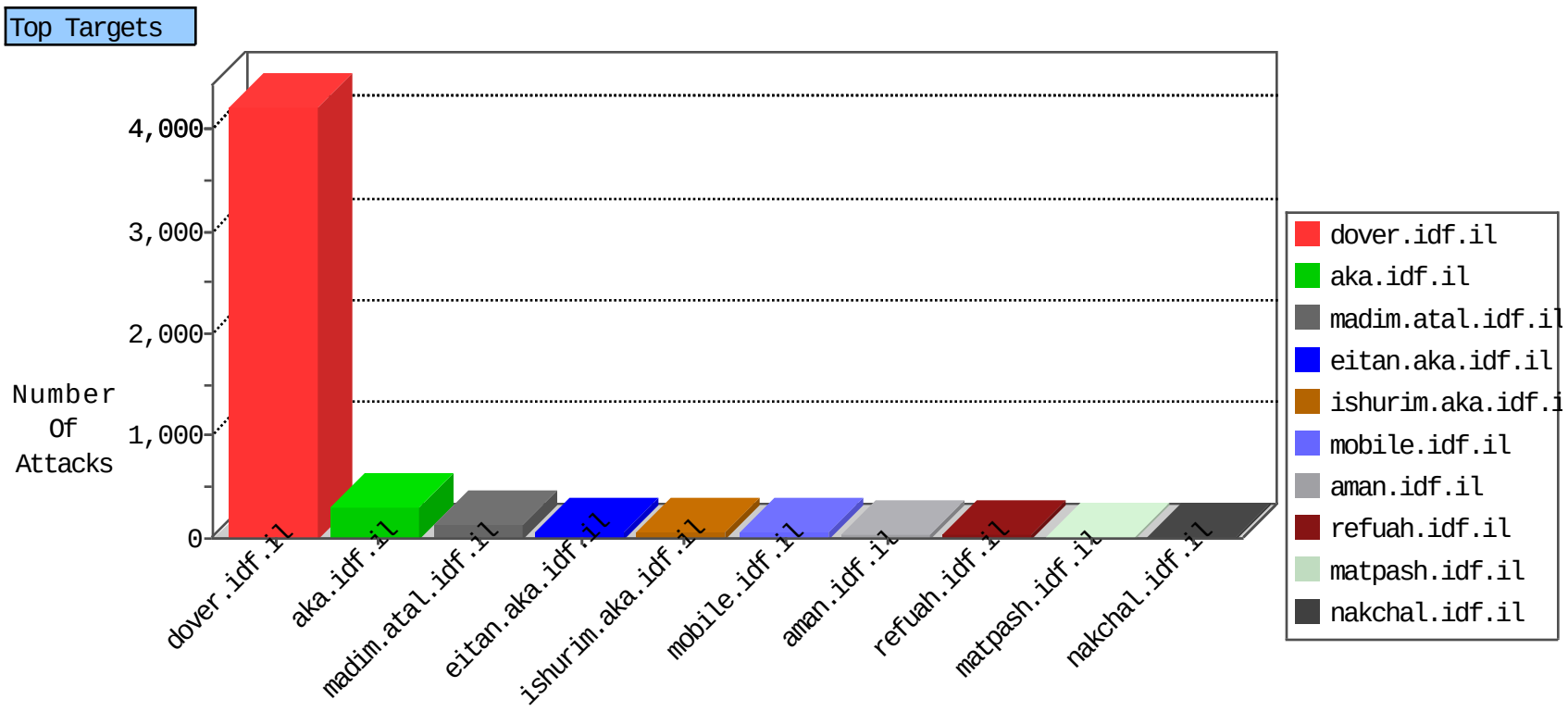
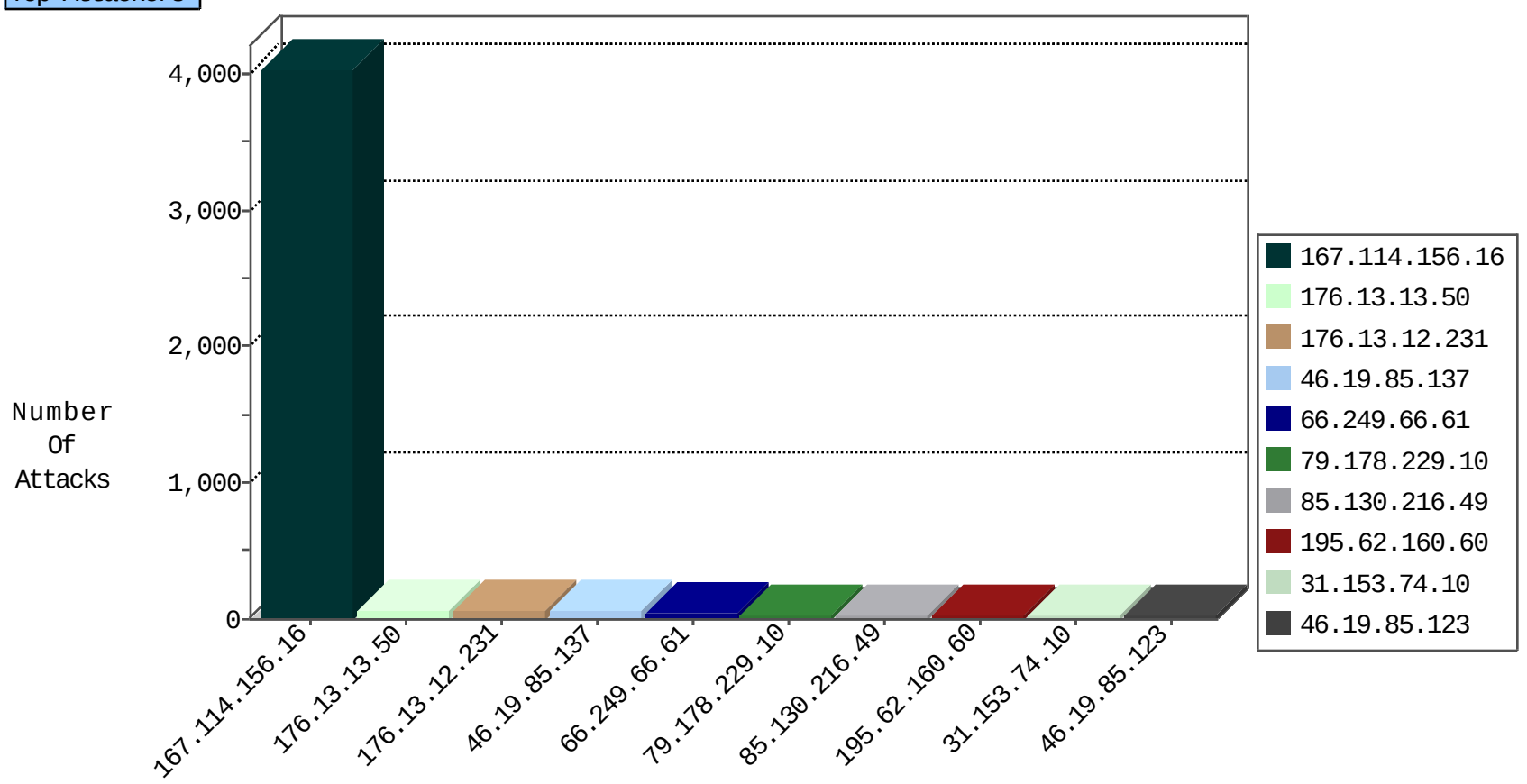
04-18-2016-16:04:08 to 04-18-2016-17:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-18-2016-16:04:08 to 04-18-2016-17:04:08

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	4027
92.82.87.8	Romania	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	11
120.132.50.135	China	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	4
204.12.196.234	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	2
74.91.20.195	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	forward	2
69.30.198.147	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
204.12.196.235	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
74.91.20.196	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
69.30.202.226	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	forward	2
74.91.20.197	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
69.197.185.20	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	2
74.91.23.109	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	2

04-18-2016-16:04:08 to 04-18-2016-17:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-18-2016-16:04:08 to 04-18-2016-17:04:08

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
2.53.183.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.110.62	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.226.45.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.71.82.42	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.229.59.35	147.237.77.216	Sweden	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.102.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.71.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.54.90.200	147.237.76.200	United States	eitan.aka.idf.il	Tehila - Perl LWP with fake user agent	1
46.117.183.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.1.99	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.106.206.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.240.250.154	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
109.64.144.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.106.125	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.40.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.30.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.12.60.100	147.237.0.16	Korea, Republic of	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
195.216.176.244	147.237.77.243	Latvia	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.246.145	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
193.169.70.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-18-2016-16:04:08 to 04-18-2016-17:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.13.50	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
79.178.229.10	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
195.62.160.60	Italy	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
31.153.74.10	Cyprus	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
2.53.30.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
82.196.42.196	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
24.114.223.254	Canada	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
79.179.113.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
46.19.85.60	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.179.23.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.53.169.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.109.147.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
85.130.216.49	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
85.130.216.49	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
87.71.82.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.138.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
85.130.216.49	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
2.53.188.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.216.49	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.177.17.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.253.210.197	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.50.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.86.77.235	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
79.177.17.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.53.17.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.179.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.244.66.127	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
61.90.57.124	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.60.41.218	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
98.116.11.127	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.108.20.110	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.27.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
80.246.137.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
185.24.76.131	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.53.149.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.46	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
82.99.20.235	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.46	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.65.99.32	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.137.207	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
185.3.147.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.80.153.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.183.213.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.68.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.136.103	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	3

04-18-2016-16:04:08 to 04-18-2016-17:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.12.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
46.19.85.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
212.199.112.144	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.199.112.144	Block	6
46.244.66.127	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	6
2.55.12.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
85.65.15.232	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	5
81.218.97.45	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	4
79.167.1.122	Greece	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	4
81.218.97.45	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/5/	Block	3
79.182.103.73	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
37.26.149.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
62.219.110.94	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/801-he/patzar.aspx	Block	2
80.246.130.231	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1072-he/nakhal.aspx	Block	2
84.94.92.240	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
37.142.64.53	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
207.46.13.31	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
79.179.179.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
69.197.185.20	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.ps780.com/	Block	1
176.228.217.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.119.112.23	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.119.112.23	Block	1
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20727-he/dover.aspx.	Block	1
81.218.97.45	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 81.218.97.45	Block	1
2.53.17.150	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
74.91.23.109	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.app-softwares.com/	Block	1
194.28.112.50	Netherlands	147.237.77.235	sviva.idf.il	Unauthorized URL Access to www.hagnas.atal.idf.il/hnap1/	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-11660-he/dover.aspx.	Block	1
66.249.66.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/tzahal-logo.jpg	Block	1
46.19.85.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.205.244.140	Greece	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
79.180.0.191	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
74.91.20.195	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to www.ps780.com/	Block	1
184.105.247.194	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.244.66.127	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	1
95.143.222.14	Russian Federation	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
2.53.188.158	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/topcap.gif	Block	1
77.237.138.202	Czech Republic	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	1
157.55.39.13	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
66.249.78.94	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
84.228.233.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.182.100.139	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	1
74.91.20.196	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.ps780.com/	Block	1
185.103.252.5	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
109.253.210.197	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
204.12.196.234	United States	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on www.369bs.com/	Block	1
176.0.31.113	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
46.119.112.23	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
212.199.112.144	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/shared/mailthisclose.png	Block	1

04-18-2016-16:04:08 to 04-18-2016-17:04:08