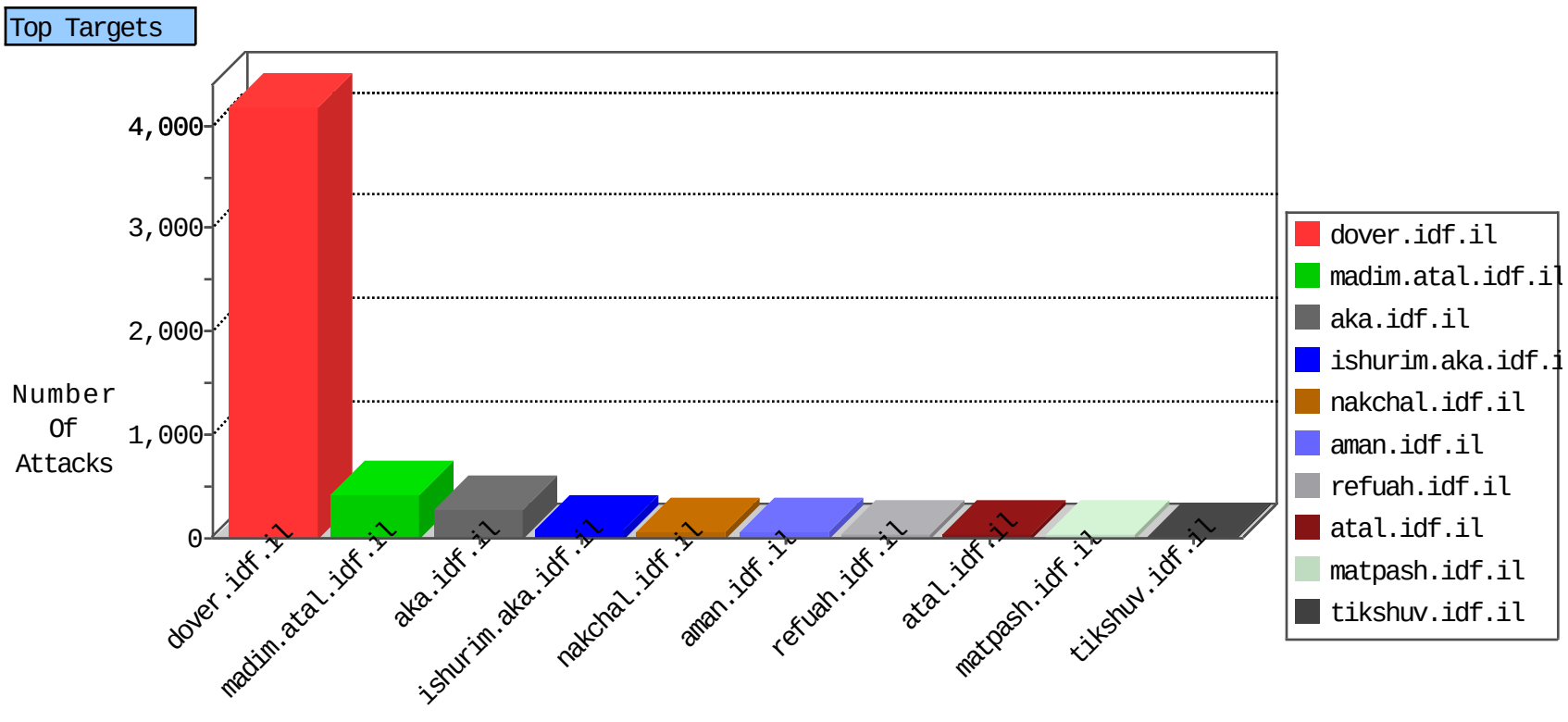
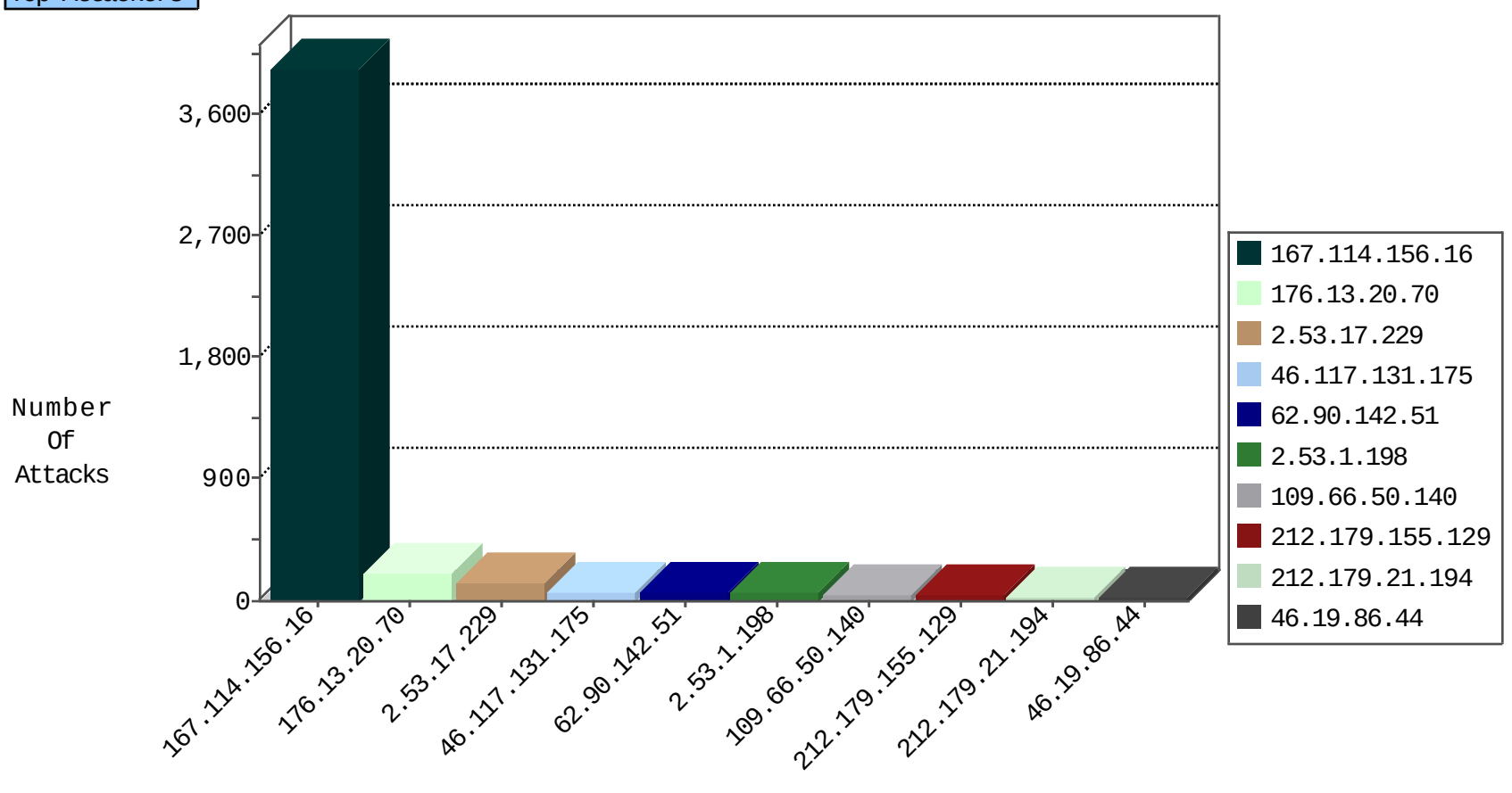
04-13-2016-14:04:00 to 04-13-2016-15:04:00

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-13-2016-14:04:00 to 04-13-2016-15:04:00

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	3944
31.168.232.150	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	12
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
185.120.126.205	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
46.19.85.187	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
192.96.201.142	United States	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1

04-13-2016-14:04:00 to 04-13-2016-15:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.120.126.205	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
84.228.16.173	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
65.55.210.190	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.25.167	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.102.9.127	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
31.168.232.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
40.77.167.92	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-13-2016-14:04:00 to 04-13-2016-15:04:00

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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
89.138.77.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.118.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.50.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.115.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.57.126	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.72.156	United States	aman.idf.il	ET DROP Dshield Block Listed Source	1
46.151.52.139	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
194.90.192.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.140.23	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.105.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.28.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.166.53.147	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
213.8.204.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.217.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.177.88.126	147.237.76.34	United States	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.140.23	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.138.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.161.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

04-13-2016-14:04:00 to 04-13-2016-15:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.117.131.175	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	55
109.66.50.140	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	51
212.179.155.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
62.90.142.51	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.44	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
46.19.86.44	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
46.19.86.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.15.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.249.156.108	Italy	147.237.77.233	atal.idf.il	drop	SAM rule	drop	12
62.90.142.51	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	12
158.58.172.238	Italy	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	11
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
84.245.33.104	Netherlands	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.118	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
212.143.148.83	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.179.21.194	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
212.179.21.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.55.151.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.187	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.93	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.24.207.52	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
62.90.142.51	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
41.33.231.82	Egypt	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	6
46.19.85.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.90.142.51	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.187.231	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
188.120.149.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	6
62.90.142.51	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
82.80.139.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.149.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
94.230.86.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.53.141.3	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.187	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.81	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.147.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.93	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.93	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.101	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.64	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.90	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.114	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.65.248.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.20.70	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
46.19.86.76	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
39.36.139.164	Pakistan	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3

04-13-2016-14:04:00 to 04-13-2016-15:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.20.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	194
2.53.17.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	139
2.53.1.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
46.116.41.11	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.116.41.11	Block	17
2.53.14.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
185.32.179.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	4
109.253.193.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
66.249.84.165	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.116.41.11	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
66.249.84.167	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
188.163.78.47	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 188.163.78.47	Block	3
80.178.98.149	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.84.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.16.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.153	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
93.172.45.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/undefined	Block	2
180.76.15.155	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9738-he/refuah.aspx	Block	1
2.53.141.3	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew	Block	1
220.181.132.216	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/home/default.aspx	Block	1
188.163.78.47	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
124.73.11.78	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/896-he/shared/usercontrols/headerupper/	Block	1
39.36.139.164	Pakistan	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/wp-login.php	Block	1
85.250.229.195	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
207.46.13.129	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/common/includes/bignewswnd.asp	Block	1
46.116.41.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58339&docid=68502&usg=alkjrhil0gtbkmbx4hmqzh72nu4qfqqzdq	Block	1
185.24.207.54	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.65.246.43	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.144.155	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
81.218.67.234	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter utm_medium in www.aka.idf.il/main/rabanut/general.aspx	None	1
149.78.210.8	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus	Block	1
41.143.75.33	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
91.200.12.85	Ukraine	147.237.72.166	aka.idf.il	Unknown Parameter amp;list in www.aka.idf.il/chinuch/klali/default.asp	None	1
212.143.164.123	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
62.0.100.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl103 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.66.50.140	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
31.154.3.222	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
66.249.78.199	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/default.asp	Block	1
157.55.39.65	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.229.27	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
213.8.44.227	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.158	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/sitemap/sitemap.aspx	Block	1
37.26.148.247	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/titlecap.png	Block	1
207.46.13.72	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.72	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

04-13-2016-14:04:00 to 04-13-2016-15:04:00