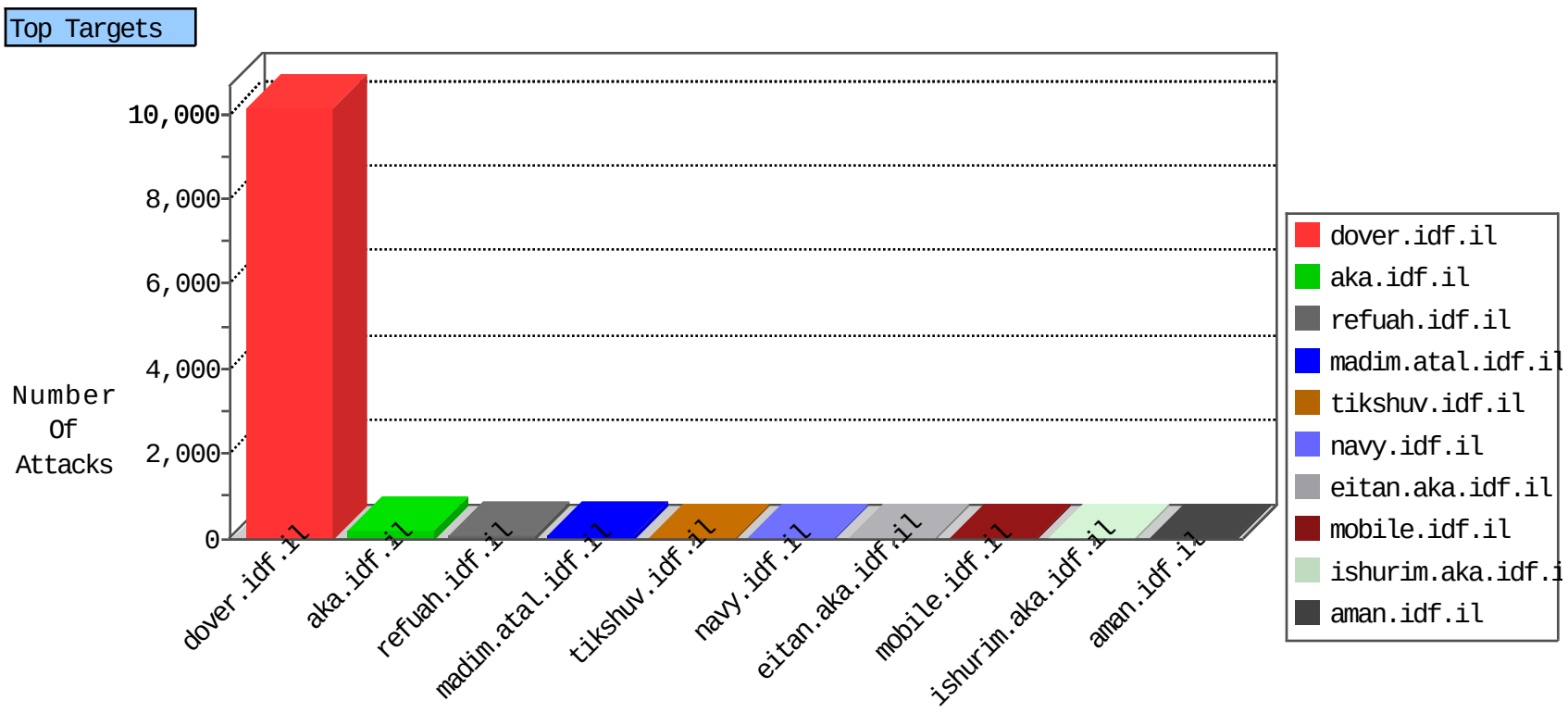
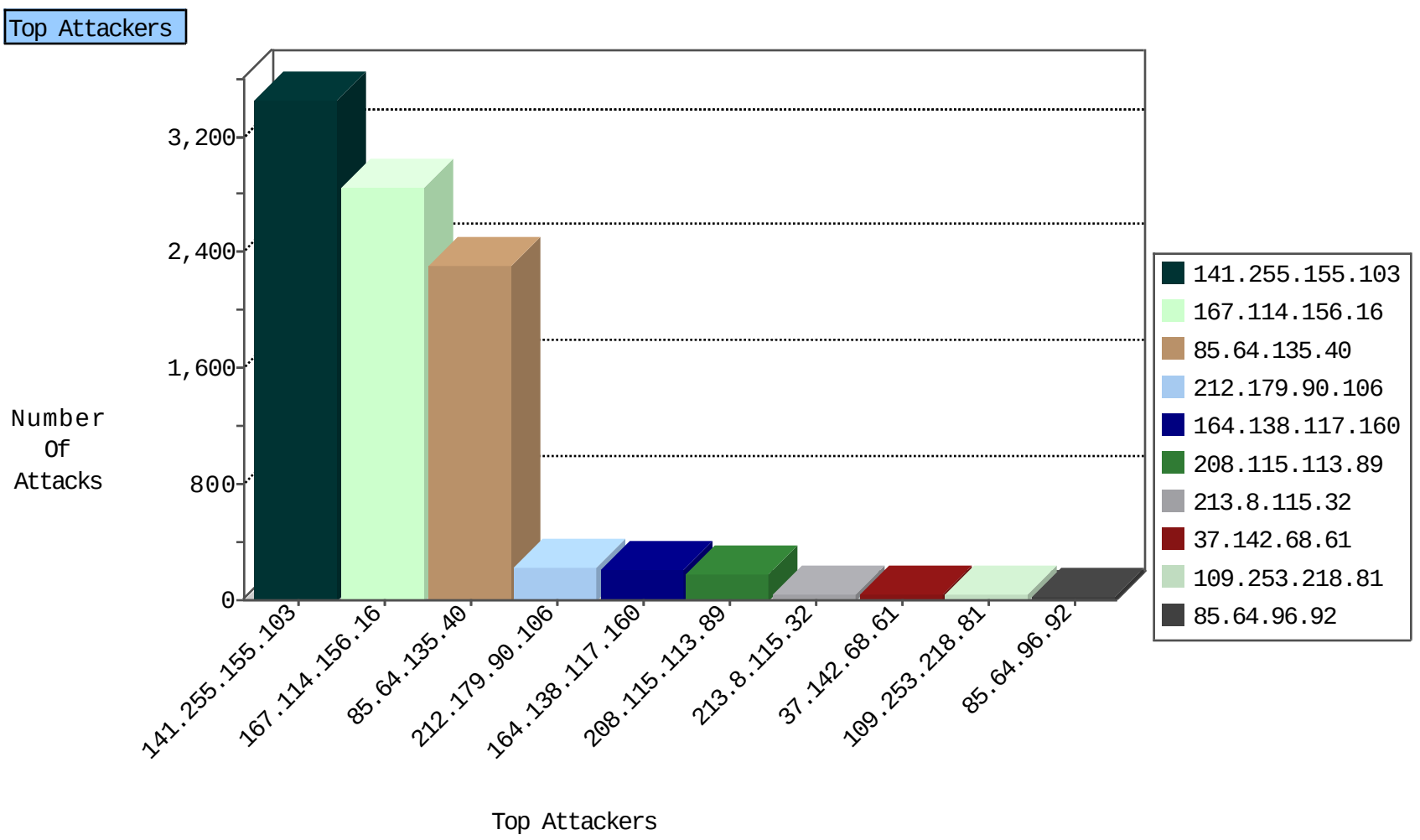
04-13-2016-15:04:00 to 04-13-2016-16:04:00

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-13-2016-15:04:00 to 04-13-2016-16:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.255.155.103	Netherlands	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3355
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	2854
141.255.155.103	Netherlands	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	885
141.255.155.103	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	632
41.102.67.46	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	2
81.218.208.46	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
62.138.3.98	Germany	147.237.76.200	eitan.aka.idf.i	Block_Ntp_All_Net	drop	1

04-13-2016-15:04:00 to 04-13-2016-16:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.205	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	22
109.65.27.223	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	8
31.168.180.232	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.177.23.20	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	4
141.255.155.103	Netherlands	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2
40.77.167.92	United States	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-13-2016-15:04:00 to 04-13-2016-16:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
109.66.72.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.70.240.19	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.87.228.70	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
46.4.79.76	147.237.77.212	Germany	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.148.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.134.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
221.203.142.131	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.77.233	United States	atal.idf.il	ET DROP Dshield Block Listed Source	1
185.130.5.217	147.237.76.198	Lithuania	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.27.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.229.91	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
221.203.142.131	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
213.8.115.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-13-2016-15:04:00 to 04-13-2016-16:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.64.135.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1967
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	226
164.138.117.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	206
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	173
213.8.115.32	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
37.142.68.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
85.64.96.92	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
109.160.160.129	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
46.19.85.189	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
5.11.47.110	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
193.43.245.250	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	13
81.218.80.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
5.102.242.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
109.186.49.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
207.244.77.144	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
213.57.21.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.182.20.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.65	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
195.110.40.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.122	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.15	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
157.55.39.217	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.82	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.116.98.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.52.100	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.179.100.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.67.14.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.114.23.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
217.132.11.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.151.38.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.179.161.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.147.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.166.100.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.26	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
79.180.111.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
82.20.234.21	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
193.43.246.250	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.218.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	12
176.13.9.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.85.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.128.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.152.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.179.115.198	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 80.179.115.198	Block	3
2.55.17.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.69.208.55	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.208.55	Block	2
79.176.82.197	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.176.136.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
131.253.25.146	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
82.80.135.182	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
82.80.135.182	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/7/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
207.46.13.129	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.129	Block	1
174.129.237.157	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
213.8.115.32	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
80.179.115.198	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
62.210.162.37	France	147.237.77.74	law.idf.il	PHP Attempt	Block	1
192.117.159.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
82.102.233.83	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
87.69.208.55	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/forms.aspx	Block	1
219.74.180.192	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.246.136.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.210.162.37	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
200.74.240.180	Panama	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
123.59.59.52	China	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to www.mafengwo.cn/1428-he/meitav.aspx	Block	1
37.26.148.203	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	1
84.94.113.54	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/yoman.asp	Block	1
184.105.139.68	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
46.19.86.25	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
31.168.6.38	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
109.67.39.56	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
82.80.135.182	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 82.80.135.182	Block	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
203.251.30.74	Korea, Republic of	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
38.111.147.84	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
84.94.158.19	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
208.115.125.36	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
80.179.115.198	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/	Block	1
192.116.227.90	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/news/pages/luxmborg.aspx	Block	1
46.121.100.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
109.67.188.138	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20063-he/idfgdover.aspx	Block	1