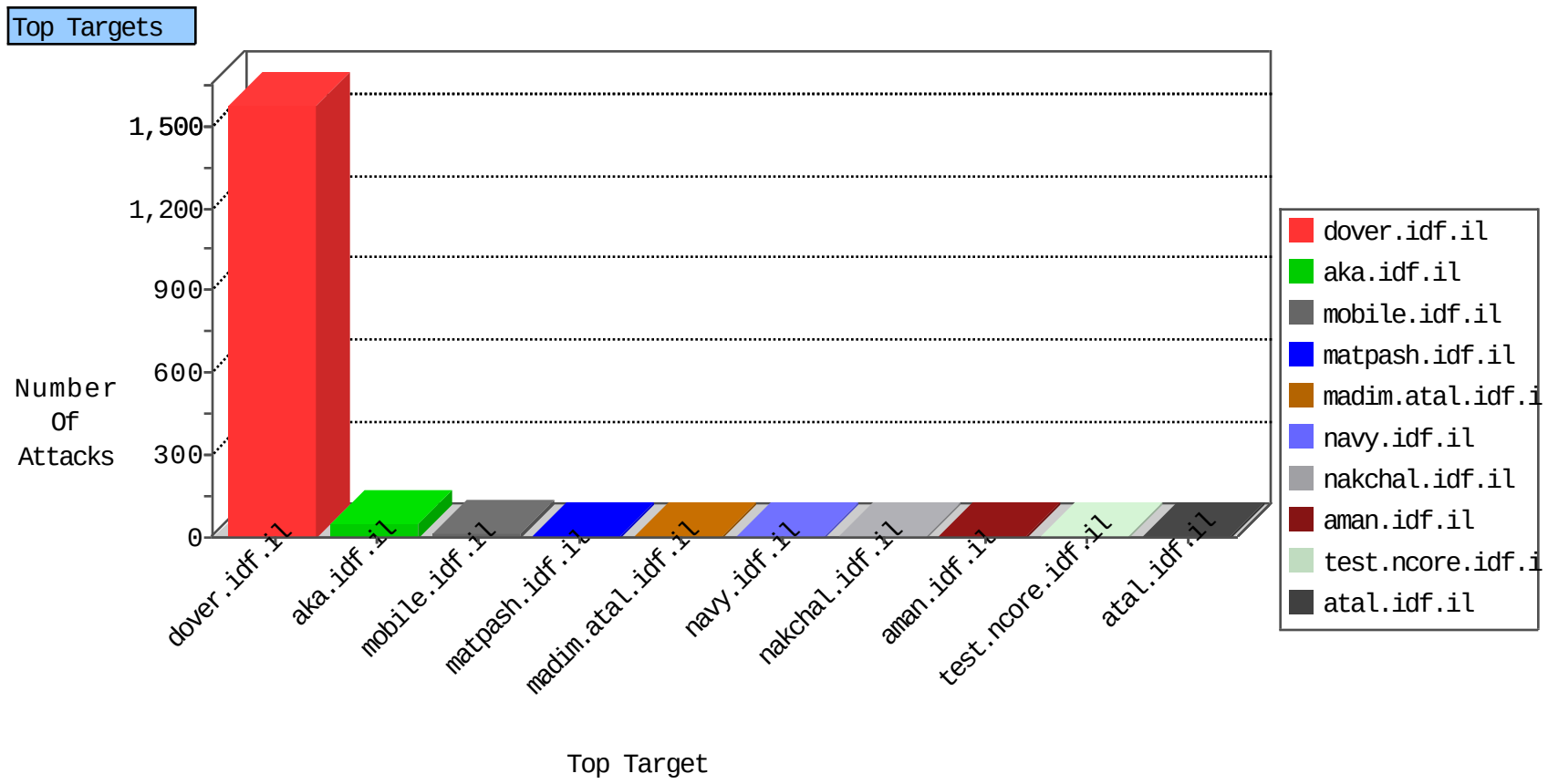
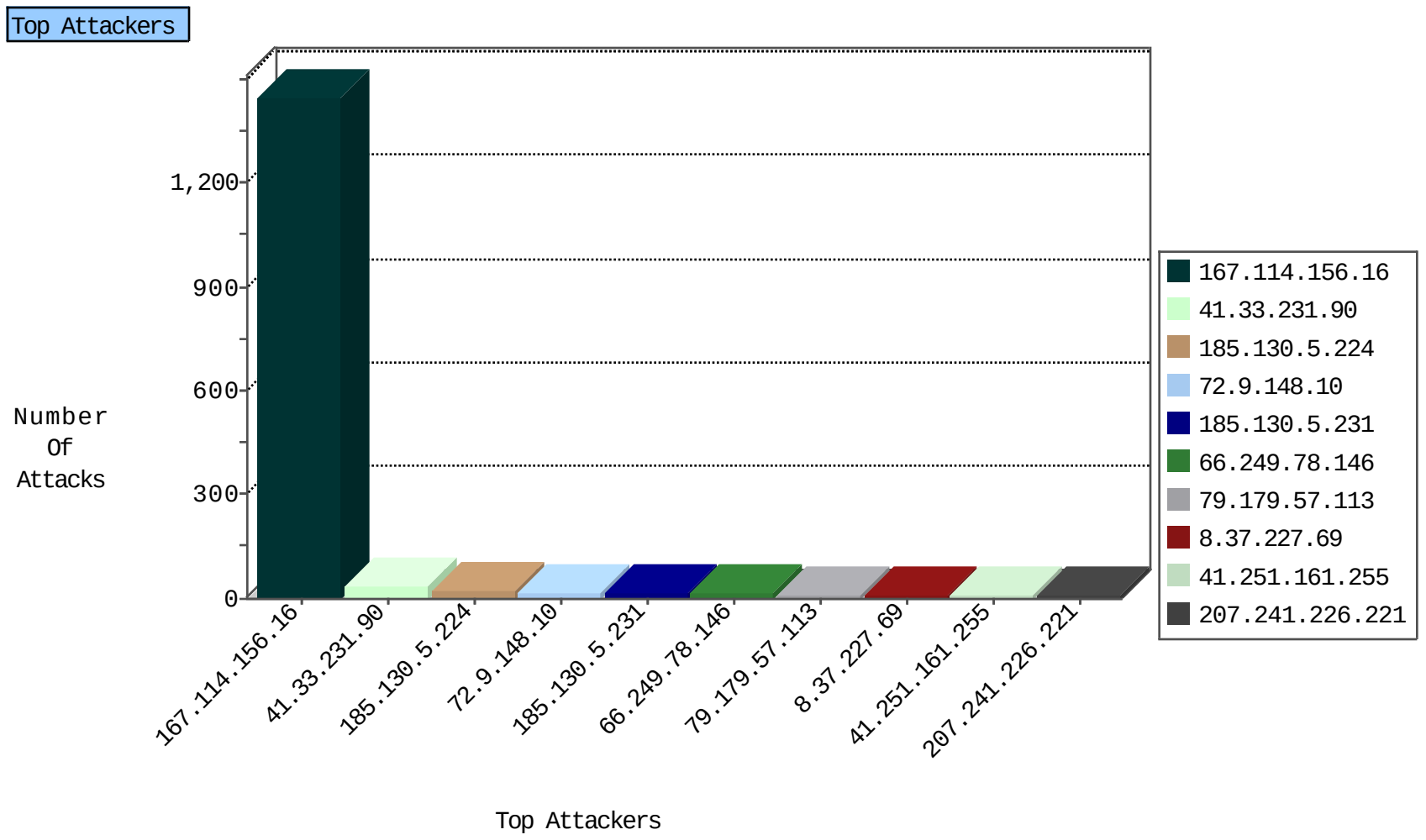
01-02-2016-02:04:07 to 01-02-2016-03:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-02-2016-02:04:07 to 01-02-2016-03:04:07

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	DOS-Tool-SwitchbladG	dest-reset	3240

01-02-2016-02:04:07 to 01-02-2016-03:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.240.213.93	United States	147.237.76.38	e.e.meitav.idf.i	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	2

01-02-2016-02:04:07 to 01-02-2016-03:04:07

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	4
41.251.161.255	147.237.76.176	Morocco	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
185.130.5.224	147.237.77.243		mobile.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
41.251.161.255	147.237.76.196	Morocco	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
41.251.161.255	147.237.0.35	Morocco	akaws.idf.il	ET SCAN Potential SSH Scan	1
41.251.161.255	147.237.0.33	Morocco	idf.il	ET SCAN Potential SSH Scan	1
41.251.161.255	147.237.0.15	Morocco	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
41.251.161.255	147.237.77.121	Morocco	e.navy.idf.il	ET SCAN Potential SSH Scan	1
41.251.161.255	147.237.0.34	Morocco	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
41.251.161.255	147.237.0.19	Morocco	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.233	United States	atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
209.126.116.147	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

01-02-2016-02:04:07 to 01-02-2016-03:04:07

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	36
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
79.179.57.113	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	10
207.241.226.221	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
73.198.146.35	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
84.228.118.172	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
198.51.240.130	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.56.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.130.5.224		147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	2
91.200.12.137	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
79.66.189.152	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
105.98.188.141	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.22.131.64	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.214.148	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.231		147.237.76.148	gqcenter.aka.idf.il	drop	SAM rule	drop	1
185.130.5.224		147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
185.130.5.224		147.237.76.44	e.refuah.idf.il	drop	SAM rule	drop	1
203.127.96.217	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
31.210.188.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.224		147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
93.189.26.18	Austria	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
80.246.137.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.130.5.224		147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
52.90.147.148	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.224		147.237.8.28	e.mobile-ks.idf.il	drop	SAM rule	drop	1
198.20.69.74	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.175.26.46	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
141.212.122.167	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.231		147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.130.5.224		147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
207.46.13.144	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
36.110.33.83	China	147.237.0.35	akaws.idf.il	drop		drop	1
185.130.5.224		147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.76.201	e.atal.idf.il	drop	SAM rule	drop	1
101.198.159.31	China	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.231		147.237.76.44	e.refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
82.166.100.163	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.130.5.224		147.237.77.212	e.dover.idf.il	drop	SAM rule	drop	1
52.90.147.148	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

01-02-2016-02:04:07 to 01-02-2016-03:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	5
185.58.226.157	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	4
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
81.218.201.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
141.212.122.160	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
74.70.101.26	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 74.70.101.26 (Open Mode)	None	1
46.166.137.204	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
157.55.39.207	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kamlar/kl	Block	1
66.249.78.201	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on nakhal.idf.il/page.asp	Block	1
66.249.73.219	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.73.219	Block	1
150.70.97.84	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
74.70.101.26	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
46.166.190.133	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/kkkkkkk=c5f35f84kkkkkkk_c5f35f84	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
207.46.13.48	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.249.73.219	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/7/3097.pdfÃ½	Block	1
2.52.129.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
150.70.97.84	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.181.71.225	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
66.249.64.186	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/1/1381.pdf	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.160	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/homepage/	Block	1
66.249.73.227	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.73.227	Block	1
2.54.146.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
150.70.173.59	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
80.246.136.169	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$emailUpdate$hiddenUpdateEmail in www.aka.idf.il/main/giyus/faq.aspx	None	1
66.249.78.187	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on nakhal.idf.il/page.asp	Block	1
198.20.69.74	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/modiin/default.aspx	Block	1
66.249.69.91	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on nakhal.idf.il/page.asp	Block	1
109.201.152.23	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/main/forums.asp	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
5.29.1.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
150.70.173.59	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.194	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on nakhal.idf.il/page.asp	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/templates/	Block	1

01-02-2016-02:04:07 to 01-02-2016-03:04:07