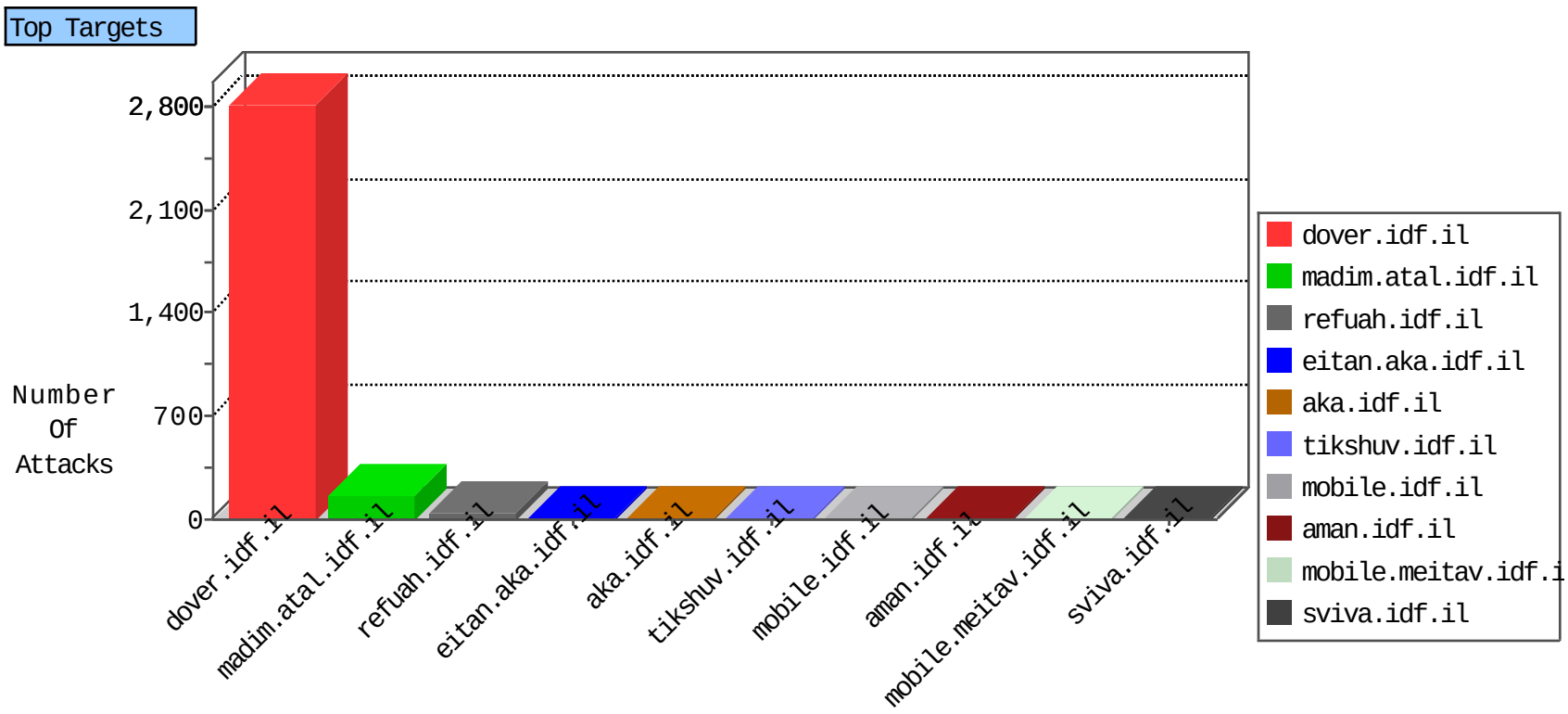
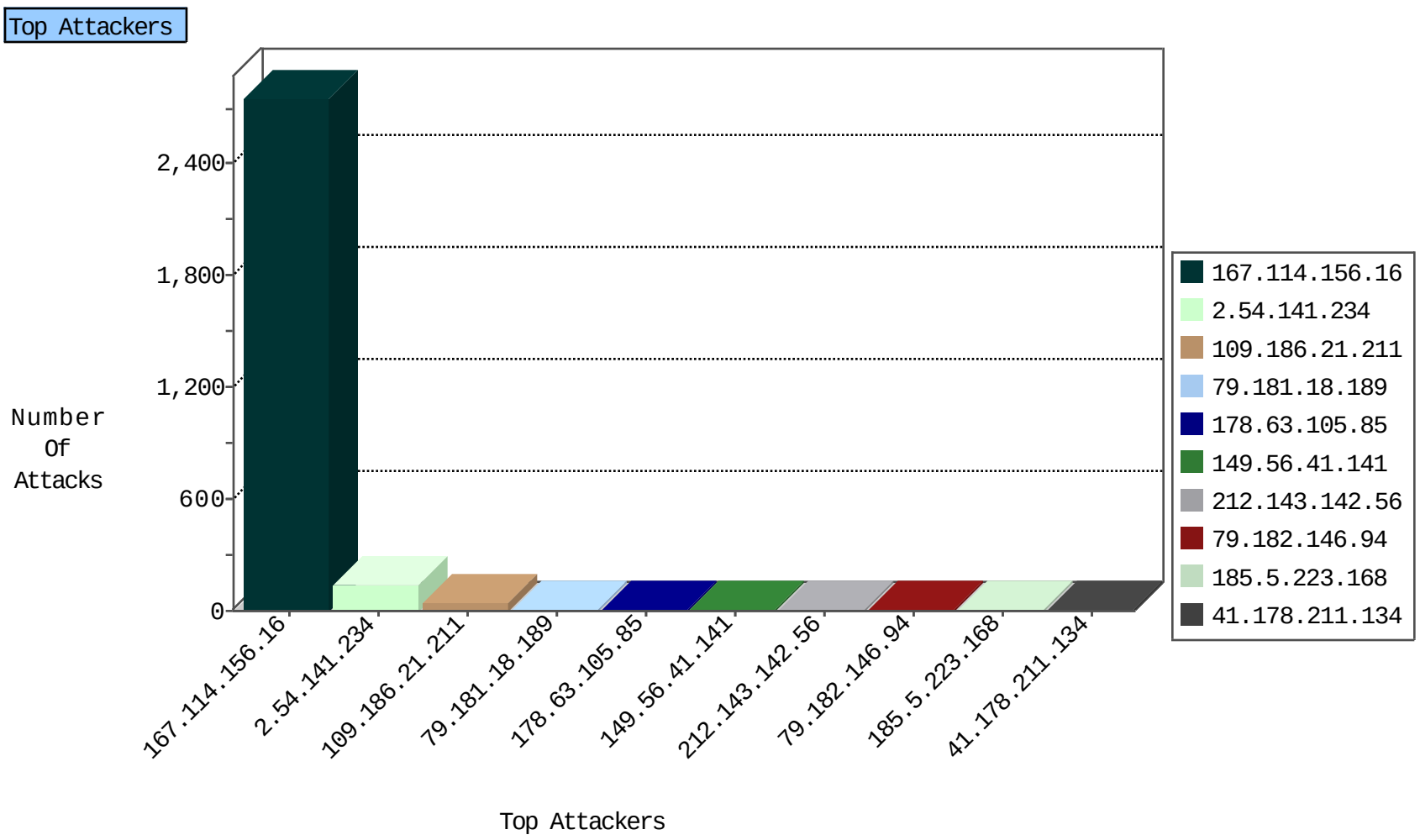
03-14-2016-01:07:09 to 03-14-2016-02:07:09

IDF Under Attack Daily Report





03-14-2016-01:07:09 to 03-14-2016-02:07:09

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	3402
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	3033
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	63
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
120.27.97.217	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2

03-14-2016-01:07:09 to 03-14-2016-02:07:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.30.24.233	United States	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	1
149.56.41.141	United States	147.237.77.216	dover.idf.il	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	1
149.56.41.141	United States	147.237.77.216	dover.idf.il	19863: HTTP: WordPress Revslider/Showbiz PHP File Upload	Block	1
149.56.41.141	United States	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	1

03-14-2016-01:07:09 to 03-14-2016-02:07:09

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
149.56.41.141	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	2
123.240.251.38	147.237.8.28	Taiwan	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.45.210.69	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
23.96.109.87	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
201.172.81.83	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
120.26.115.52	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
104.45.210.69	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -f -sS	1
201.172.81.83	147.237.76.196	Mexico	e.sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.20.69.98	147.237.77.235	United States	sviva.idf.il	ET DROP Dshield Block Listed Source	1
185.98.87.187	147.237.77.243		mobile.idf.il	ET SCAN NMAP -sS window 1024	1

03-14-2016-01:07:09 to 03-14-2016-02:07:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.186.21.211	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.181.18.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.146.94	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.138.180.82	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.178.211.134	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.30.25.12	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.253.147.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.142.34	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
149.78.40.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.66.60.75	Denmark	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	2
173.68.118.204	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
79.178.196.147	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.5.223.168	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	2
212.199.121.158	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
73.231.246.63	United States	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	2
157.55.2.158	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
84.94.26.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
70.209.60.103	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
172.245.104.223	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	1
141.212.122.170	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.5.223.168	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
77.127.215.190	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
159.226.95.66	China	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.77	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
207.46.13.87	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.94.26.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
178.63.105.85	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
71.233.107.249	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.173	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.5.223.168	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
178.63.105.85	Germany	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
5.29.203.75	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.78	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
71.233.107.249	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
178.63.105.85	Germany	147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	1
141.212.122.174	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.65	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.27.105.126	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.29.203.75	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.79	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.5.223.168	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.141.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	141
79.181.18.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
149.56.41.141	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
37.26.149.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.24.207.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.223.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.181.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.20.157	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
104.131.69.61	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 104.131.69.61	Block	1
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/3480.jpg	Block	1
183.206.175.39	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 183.206.175.39	Block	1
131.253.25.164	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.82.65.82	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.65.188	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
149.56.41.141	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 149.56.41.141	Block	1
104.131.69.61	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/14-he	Block	1
67.86.244.110	United States	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
183.206.175.39	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/editor/editor/	Block	1
41.47.149.233	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
131.253.25.227	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.71.9.228	Israel	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
173.68.118.204	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.186.21.211	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
77.75.79.101	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
41.47.149.233	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
141.212.122.64	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /x	Block	1
87.71.9.228	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
31.13.100.114	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/&-h=uaqhyd1x0&enc=azmn-iafhix46vm4yxyrdikuc-ev99ae3lsosjivbqybpi-nrlepiovaxfgebbkkzvt-87yfmfzeqmrg4lnyaazb-xzqb7pc0lv4juukeff0p-nvtif9xfdbywtixzmqym-qnk1_e0jzzxdj8hpozqv-vcrthkvbzzr5ne6l1zce-m4h3bhf0e9eqv--tzlio-o16sqfb40ic&s=1لينكا	Block	1
77.127.215.190	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
149.56.41.141	United States	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
87.255.94.119	Moldova, Republic of	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8583-he/refuah.aspx	Block	1
31.13.112.119	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/&-h=uaqhyd1x0&enc=azmn-iafhix46vm4yxyrdikuc-ev99ae3lsosjivbqybpi-nrlepiovaxfgebbkkzvt-87yfmfzeqmrg4lnyaazb-xzqb7pc0lv4juukeff0p-nvtif9xfdbywtixzmqym-qnk1_e0jzzxdj8hpozqv-vcrthkvbzzr5ne6l1zce-m4h3bhf0e9eqv--tzlio-o16sqfb40ic&s=1لينكا	Block	1
183.206.175.39	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/editor/editor/	Block	1
120.27.97.217	China	147.237.77.216	dover.idf.il	Malformed URL search.yahoo.com:443	Block	1

03-14-2016-01:07:09 to 03-14-2016-02:07:09