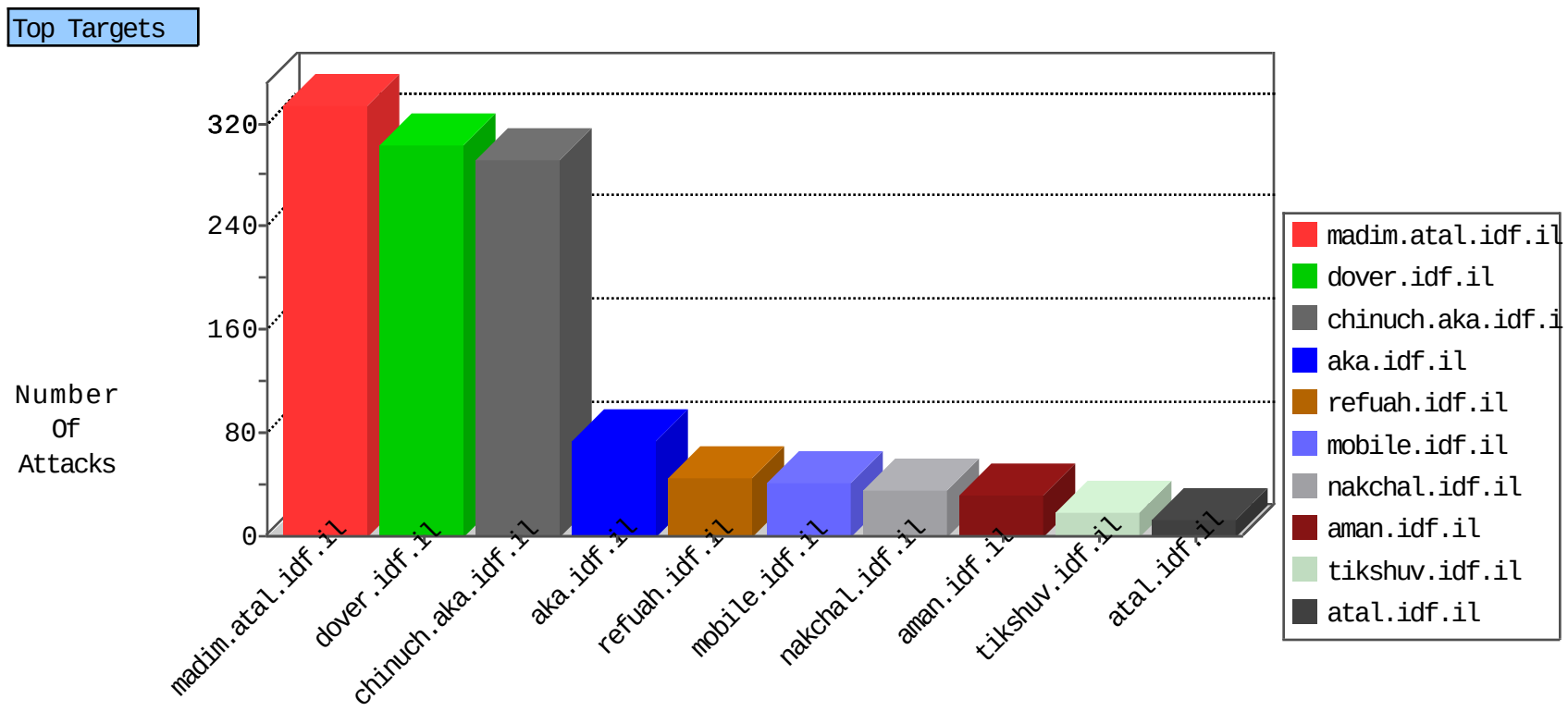
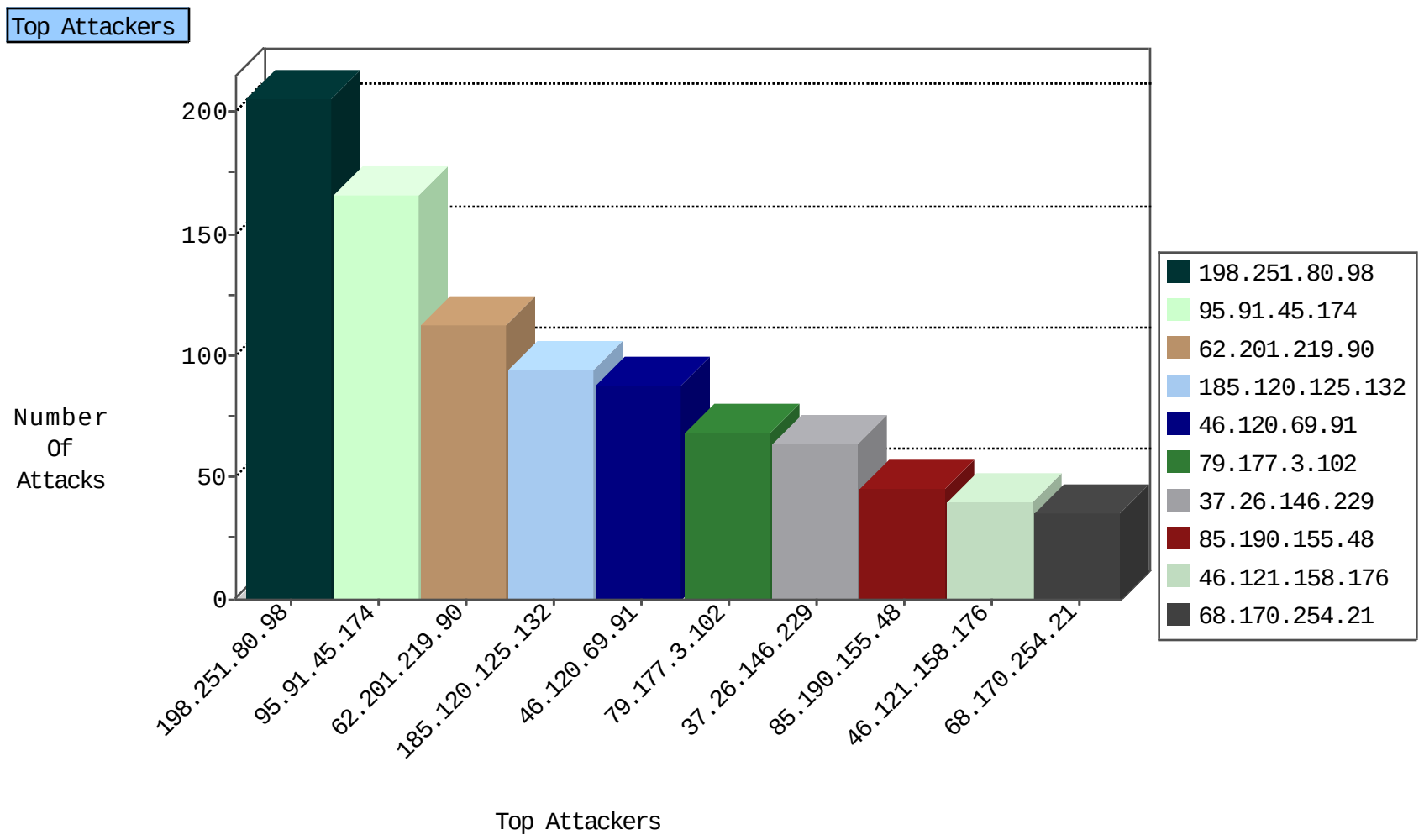
09-24-2016-22:04:07 to 09-24-2016-23:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-24-2016-22:04:07 to 09-24-2016-23:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.186.250.82	Germany	147.237.77.212	e.dover.idf.il	L4 Source or Dest Port Zero	drop	1
109.236.86.32	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
31.204.128.22	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
123.59.59.52	China	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
31.204.128.22	Netherlands	147.237.76.202	e.halag.idf.il	Black List	drop	1
104.238.146.238	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

09-24-2016-22:04:07 to 09-24-2016-23:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.91.45.174	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	78
95.91.45.174	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	38
95.91.45.174	Germany	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	31
95.91.45.174	Germany	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Permit	6
95.91.45.174	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	4
95.91.45.174	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	4
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
46.165.197.141	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
95.91.45.174	Germany	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Permit	2
46.183.223.232	Latvia	147.237.77.216	dover.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1

09-24-2016-22:04:07 to 09-24-2016-23:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
59.59.254.132	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
123.176.46.20	147.237.72.167	India	ishurim.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
85.64.229.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
78.129.171.173	147.237.8.27	United Kingdom	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.243	China	mobile.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.65	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
198.20.69.98	147.237.72.166	United States	aka.idf.il	ET DROP Dshield Block Listed Source	1
85.65.24.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
78.129.171.173	147.237.77.176	United Kingdom	matpash.idf.il	ET SCAN Potential SSH Scan	1
62.201.219.90	147.237.77.216	Iraq	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	147.237.72.166	China	aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.65	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
41.215.36.46	147.237.76.38	Kenya	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.240.243	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

09-24-2016-22:04:07 to 09-24-2016-23:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	49
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	49
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	49
68.170.254.21	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	35
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	32
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	27
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
85.65.4.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
141.226.217.64	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
82.173.207.83	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
85.190.155.48	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
85.190.155.48	Germany	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	10
85.190.155.48	Germany	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	10
85.190.155.48	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
46.121.158.176	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.121.158.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
92.207.200.42	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
82.113.106.192	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.68.44.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
185.32.179.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.121.158.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
85.190.155.48	Germany	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.67.53.177	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
89.237.121.61	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
131.253.25.194	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
89.237.121.61	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.121.158.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
66.102.9.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.64.181.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.121.158.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
141.226.218.58	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.121.158.176	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
77.124.15.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.58.69	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.121.158.176	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.80	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.29.179.28	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.53.15.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.253.230.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
85.65.237.61	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.69.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
185.120.125.132	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	74
79.177.3.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
37.26.146.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
185.120.125.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
95.86.74.39	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	7
217.132.21.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
79.180.221.214	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
85.65.164.250	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
85.65.186.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.20.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.166.13	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.55.166.13	Block	2
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/3350.jpg	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	1
31.154.81.55	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
77.138.62.74	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/faq.aspx	Block	1
66.249.66.243	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
157.55.39.1	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
46.120.239.229	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
2.55.166.13	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
66.249.75.187	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/m/	Block	1
66.249.64.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/assetlinks.json	Block	1
89.139.102.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.124.177	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.69.106	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/iturim/asp/displayallsoldiers.asp	Block	1
157.55.39.167	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
46.121.79.22	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
79.181.39.222	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
5.28.168.135	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
66.249.76.114	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
66.249.64.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/apple-app-site-association	Block	1
207.46.13.148	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
46.19.86.40	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.241.137	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.241.137	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	1
46.183.223.232	Latvia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/phppath/php	Block	1
24.222.93.38	Canada	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
84.111.109.138	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jeninkilled/stn	Block	1
66.249.65.156	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
109.63.167.83	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Unauthorized Method POST for www.chinuch.aka.idf.il/894-he/chinuch.aspx	None	1
77.139.241.137	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
185.27.105.69	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/'	Block	1
31.154.81.55	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-ar/cogat.aspx	Block	1
66.249.66.218	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/templates/searchresults/searchresults.aspx	Block	1
109.64.182.146	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1