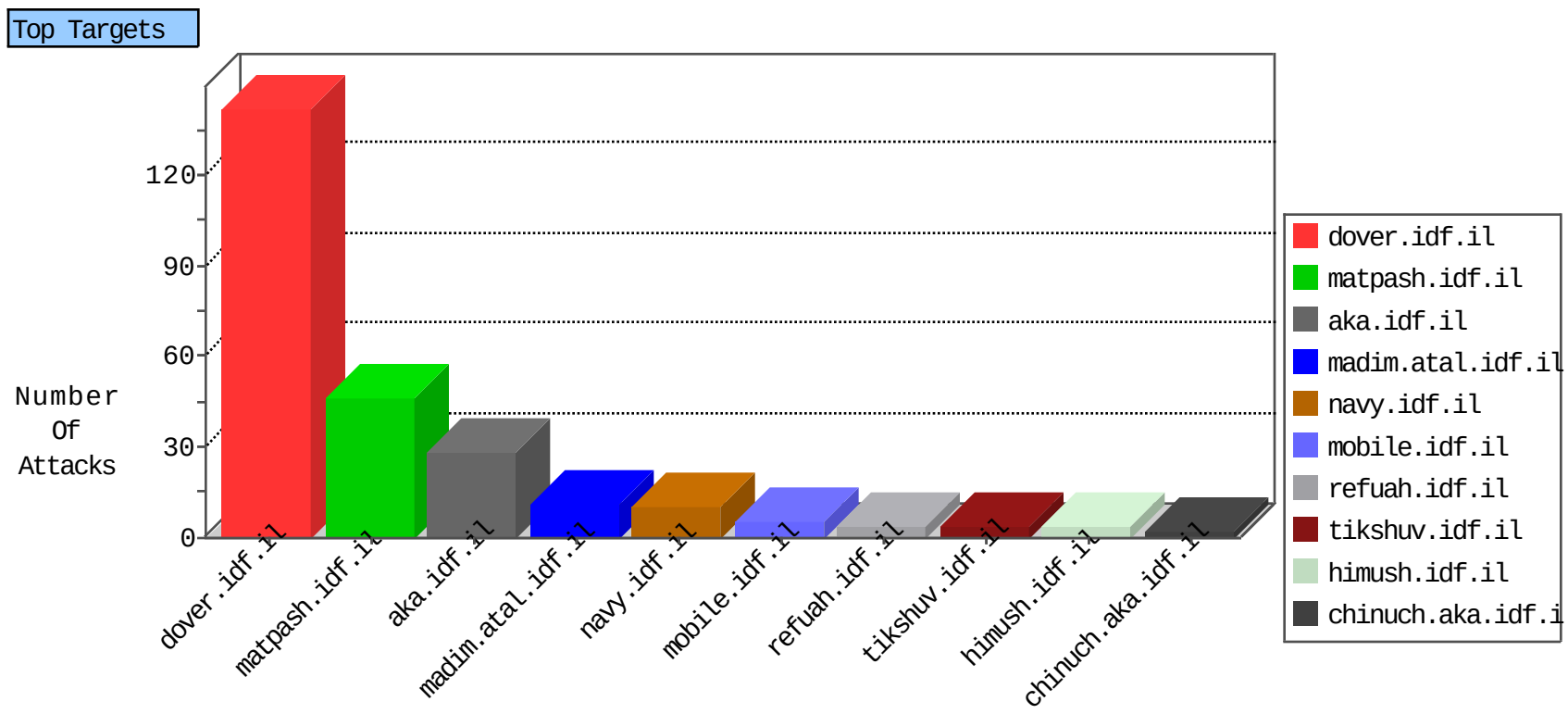
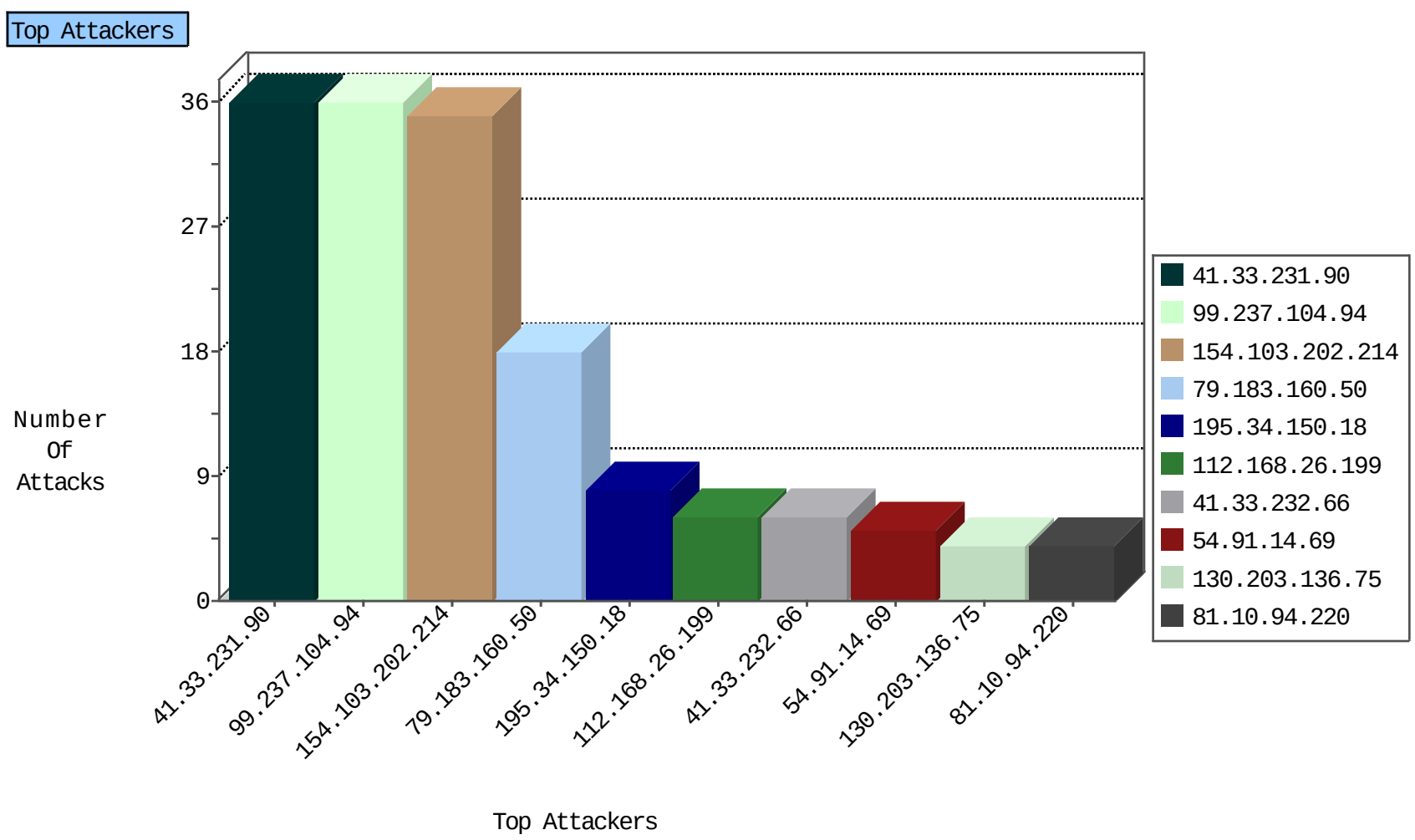
02-12-2016-06:04:03 to 02-12-2016-07:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-12-2016-06:04:03 to 02-12-2016-07:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2
185.130.5.224		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
115.239.228.10	China	147.237.76.200	eitan.aka.idf.il	JLM_Under_Attack_Con_Http	drop	1
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1

02-12-2016-06:04:03 to 02-12-2016-07:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-12-2016-06:04:03 to 02-12-2016-07:04:03

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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.65.224	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
198.12.82.58	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
77.148.66.73	147.237.76.177	France	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
187.95.18.51	147.237.77.205	Brazil	prisha.idf.il	ET SCAN Potential SSH Scan	1
112.196.49.101	147.237.77.243	India	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
112.196.49.101	147.237.77.243	India	mobile.idf.il	ET SCAN NMAP -f -sS	1
112.168.26.199	147.237.76.44	Korea, Republic of	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
112.168.26.199	147.237.0.35	Korea, Republic of	akaws.idf.il	ET SCAN Potential SSH Scan	1
112.168.26.199	147.237.0.16	Korea, Republic of	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.161.31.82	147.237.76.30	Taiwan	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.193	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
198.12.82.58	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
77.148.66.73	147.237.76.177	France	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
187.95.18.51	147.237.77.212	Brazil	e.dover.idf.il	ET SCAN Potential SSH Scan	1
115.28.247.220	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
14.54.113.150	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.196.49.101	147.237.77.243	India	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
112.168.26.199	147.237.76.196	Korea, Republic of	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
112.168.26.199	147.237.76.42	Korea, Republic of	refuah.idf.il	ET SCAN Potential SSH Scan	1
112.168.26.199	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.72.217	Canada	e.idf.il	ET SCAN NMAP -sS window 3072	1

02-12-2016-06:04:03 to 02-12-2016-07:04:03

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	32
154.103.202.214	Sudan	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	28
99.237.104.94	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
99.237.104.94	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
79.183.160.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
79.183.160.50	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
130.203.136.75	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
181.197.160.142	Panama	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.54.141.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.55.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
154.103.202.214	Sudan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.94.36.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
184.170.76.234	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
54.91.14.69	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
76.127.35.216	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
54.91.14.69	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
115.230.124.164	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.78	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.44	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.224	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
50.19.185.198	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
134.170.12.185	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
77.237.138.202	Czech Republic	147.237.77.234	halag.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
54.163.91.231	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
182.118.21.232	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
123.126.113.80	China	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
218.22.211.69	China	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.50	United States	147.237.0.33	idf.il	drop		drop	1
184.105.247.232	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
54.82.30.209	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
24.196.156.27	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
198.1.101.123	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.75	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
42.62.74.74	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
123.126.113.80	China	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
218.22.211.69	China	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.50	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.170.76.234	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
54.82.30.209	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
24.196.156.27	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.217.218	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
79.182.11.117	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.1.101.123	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1

02-12-2016-06:04:03 to 02-12-2016-07:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
154.103.202.214	Sudan	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 154.103.202.214	Block	3
37.26.148.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.85	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
46.120.199.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
81.10.94.220	Egypt	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
207.46.13.31	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.31	Block	2
81.10.94.220	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	2
54.91.14.69	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/brothers/skira/default.asp	Block	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	1
40.77.167.68	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/sachar/faq.aspx	None	1
123.126.113.80	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/faq.aspx	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
184.105.247.196	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
79.182.108.92	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	1
54.91.14.69	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
207.46.13.152	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
41.130.180.60	Egypt	147.237.76.30	himush.idf.il	PHP Attempt	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
50.19.185.198	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/brothers/skira/default.asp	Block	1
195.138.85.250	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/sendtofriend.aspx?&amp	Block	1
66.102.9.91	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1294-en/www.idf.il/english	Block	1
208.113.198.103	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/blog/wp-admin/	Block	1
41.130.180.60	Egypt	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/xmlrpc.php	Block	1
154.103.202.214	Sudan	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.65.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17802-he/dover.aspx	Block	1
50.62.176.35	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/old/wp-admin/	Block	1
66.102.9.101	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
213.8.204.18	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
45.55.42.203		147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/3249.jpg	Block	1
54.82.30.209	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/brothers/skira/default.asp	Block	1
207.46.13.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/&q=Ø§Ù„Ø§Ø³Ø±Ø§Ø¦ÙŠÙ„ÙŠ &sa=x&ei=oed5t-rlm4-r-gbqp8hkbg&ved=0cc0qfjag	Block	1
83.169.10.185	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.64.181	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
213.8.204.18	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
182.118.21.250	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.237.138.202	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1

02-12-2016-06:04:03 to 02-12-2016-07:04:03