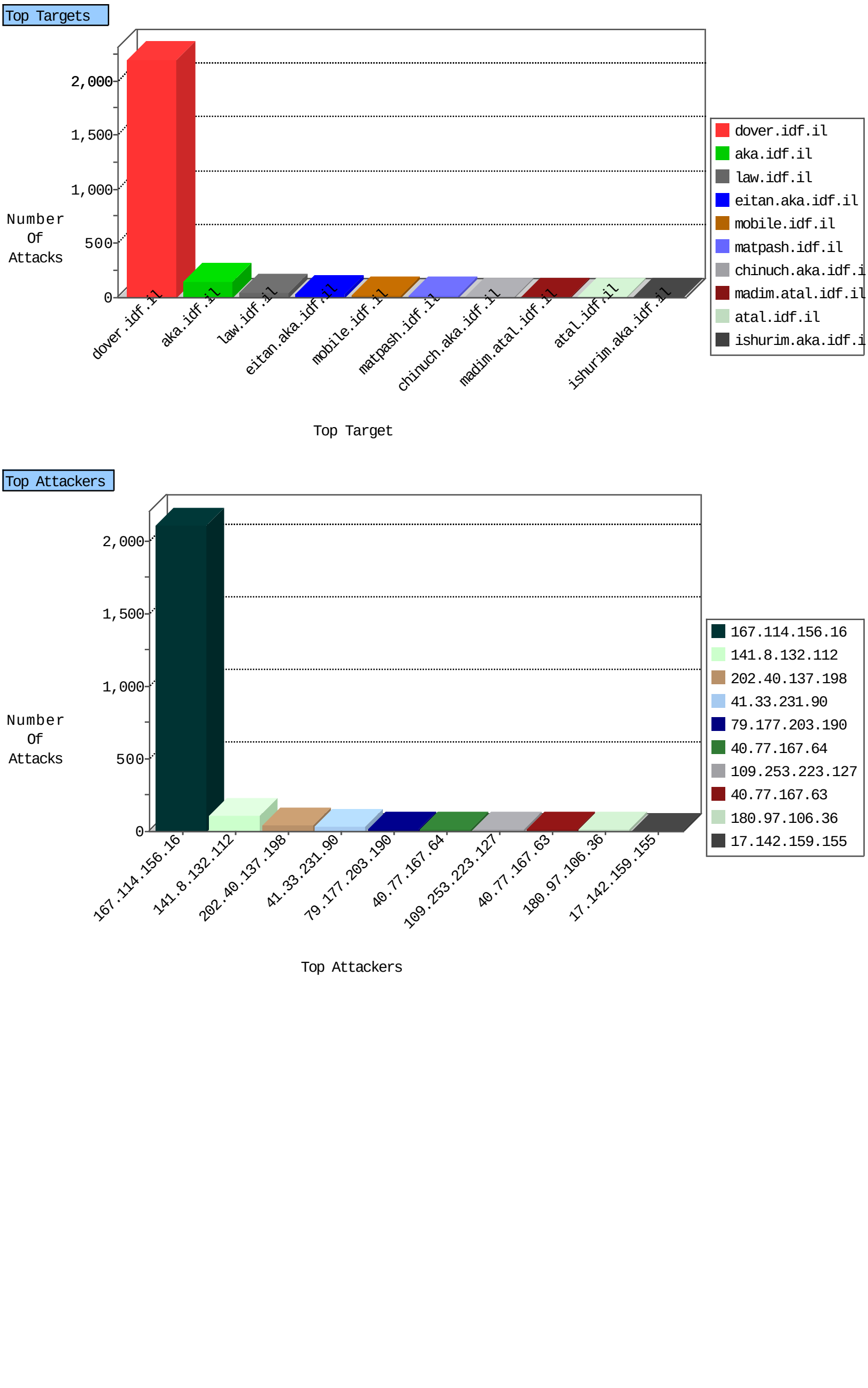
01-22-2016-06:04:06 to 01-22-2016-07:04:06

IDF Under Attack Daily Report



01-22-2016-06:04:06 to 01-22-2016-07:04:06

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	3060
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2
180.97.106.161	China	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1
180.97.106.36	China	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
79.176.4.235	Israel	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.37	China	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	drop	1
180.97.106.36	China	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
180.97.106.161	China	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
180.97.106.36	China	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
80.82.64.37	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.161	China	147.237.0.19	madim.atal.idf.il	block-sp-traf1	drop	1
180.97.106.36	China	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
180.97.106.161	China	147.237.77.170	maarachot.idf.il	block-sp-traf1	drop	1
180.97.106.36	China	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
180.97.106.161	China	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	drop	1
180.97.106.36	China	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
180.97.106.162	China	147.237.0.34	tikshuv.idf.il	block-sp-traf1	drop	1
180.97.106.37	China	147.237.76.31	nakchal.idf.il	block-sp-traf1	drop	1
180.97.106.36	China	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	drop	1

01-22-2016-06:04:06 to 01-22-2016-07:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.159	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
177.185.192.77	Brazil	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
178.151.143.163	Ukraine	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1

01-22-2016-06:04:06 to 01-22-2016-07:04:06

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
177.185.192.77	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	3
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
172.98.200.237	147.237.72.217		e.idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
98.119.105.221	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -f -sS	1
23.101.3.156	147.237.77.19	Hong Kong	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.0.33	Latvia	idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.0.16	Latvia	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
172.98.200.237	147.237.72.217		e.idf.il	ET SCAN NMAP -sS window 4096	1
172.98.200.237	147.237.72.217		e.idf.il	ET SCAN NMAP -f -sS	1
98.119.105.221	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
23.101.3.156	147.237.77.170	Hong Kong	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.0.34	Latvia	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
23.101.3.156	147.237.76.201	Hong Kong	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.0.19	Latvia	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

01-22-2016-06:04:06 to 01-22-2016-07:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
202.40.137.198	Hong Kong	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	35
79.177.203.190	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
40.77.167.64	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
109.253.223.127	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
202.40.137.198	Hong Kong	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
40.77.167.63	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
17.142.159.155	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
166.172.62.191	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
40.77.167.57	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
84.108.195.179	Israel	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
157.55.39.173	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.183.241.73	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.142.1	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.124	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	3
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.121.123.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.78.153	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
112.198.75.66	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
207.46.13.149	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
84.111.226.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
159.8.109.19	Netherlands	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
112.198.75.66	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.203	United States	147.237.0.33	idf.il	drop		drop	1
46.19.86.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.97.106.36	China	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
89.108.144.114	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
192.0.112.18	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.97.106.162	China	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
112.198.75.66	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
207.46.13.146	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	alert	1
184.105.247.203	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.97.106.36	China	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	1
216.218.206.91	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
184.66.143.6	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
112.198.75.66	Philippines	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
207.46.13.146	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
80.246.136.131	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.211	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
65.55.212.67	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
180.97.106.36	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
157.55.39.77	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.95	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
198.20.70.114	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

01-22-2016-06:04:06 to 01-22-2016-07:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.111.226.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.111.226.234	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
109.253.213.114	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	2
5.29.117.24	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
207.241.229.149	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
157.55.39.85	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
87.226.83.73	Latvia	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
31.148.219.165	Netherlands	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
157.55.39.214	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	1
69.58.178.59	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
31.148.219.165	Netherlands	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/administrator/	Block	1
166.62.100.202	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/faq.aspx	Block	1
207.46.13.36	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	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
40.77.167.63	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/registrationwizard/register.aspx	Block	1
180.76.15.12	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
207.46.13.149	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/1056-he.patzar.aspx	Block	1
40.77.167.64	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/misrot.aspx	Block	1
180.76.15.145	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9236-he/refuah.aspx	Block	1
87.226.83.73	Latvia	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1

01-22-2016-06:04:06 to 01-22-2016-07:04:06