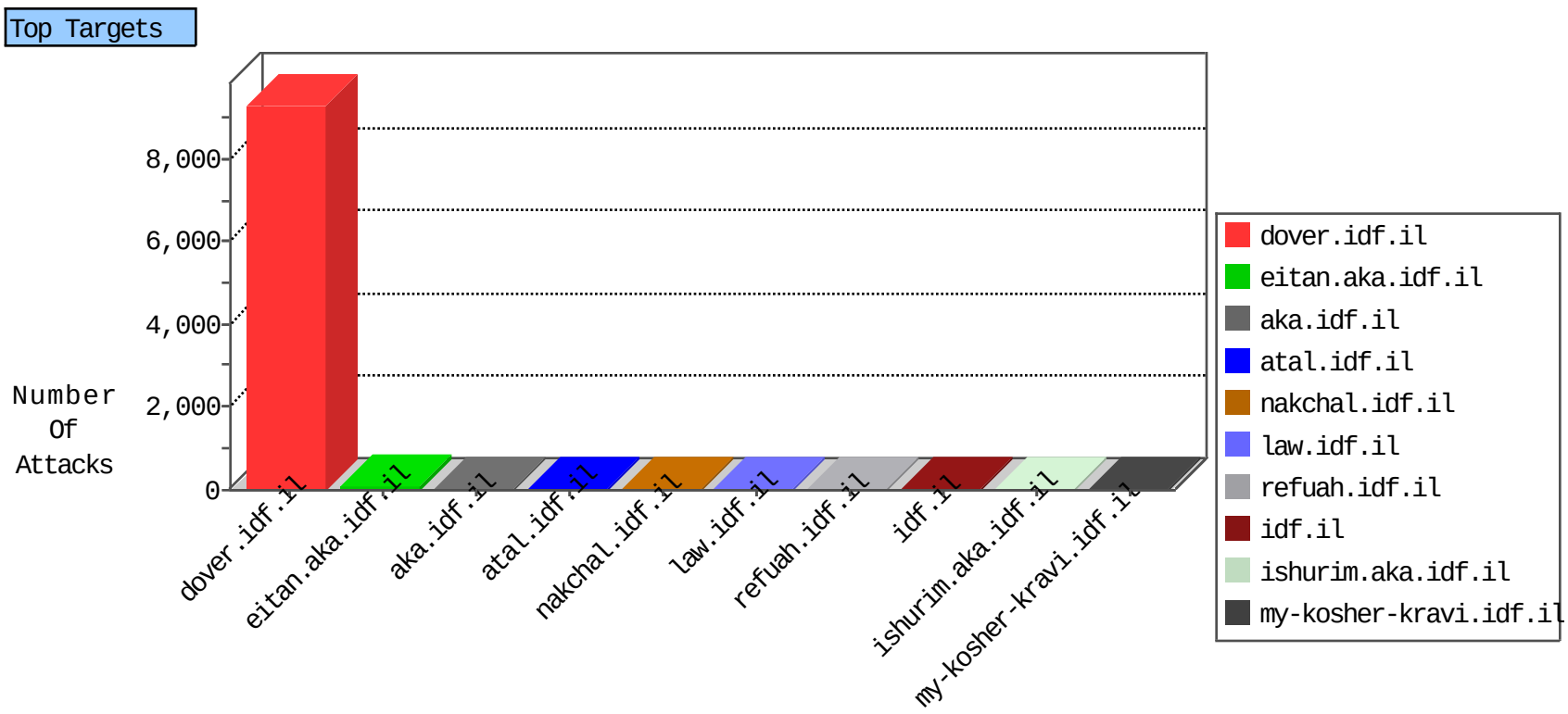
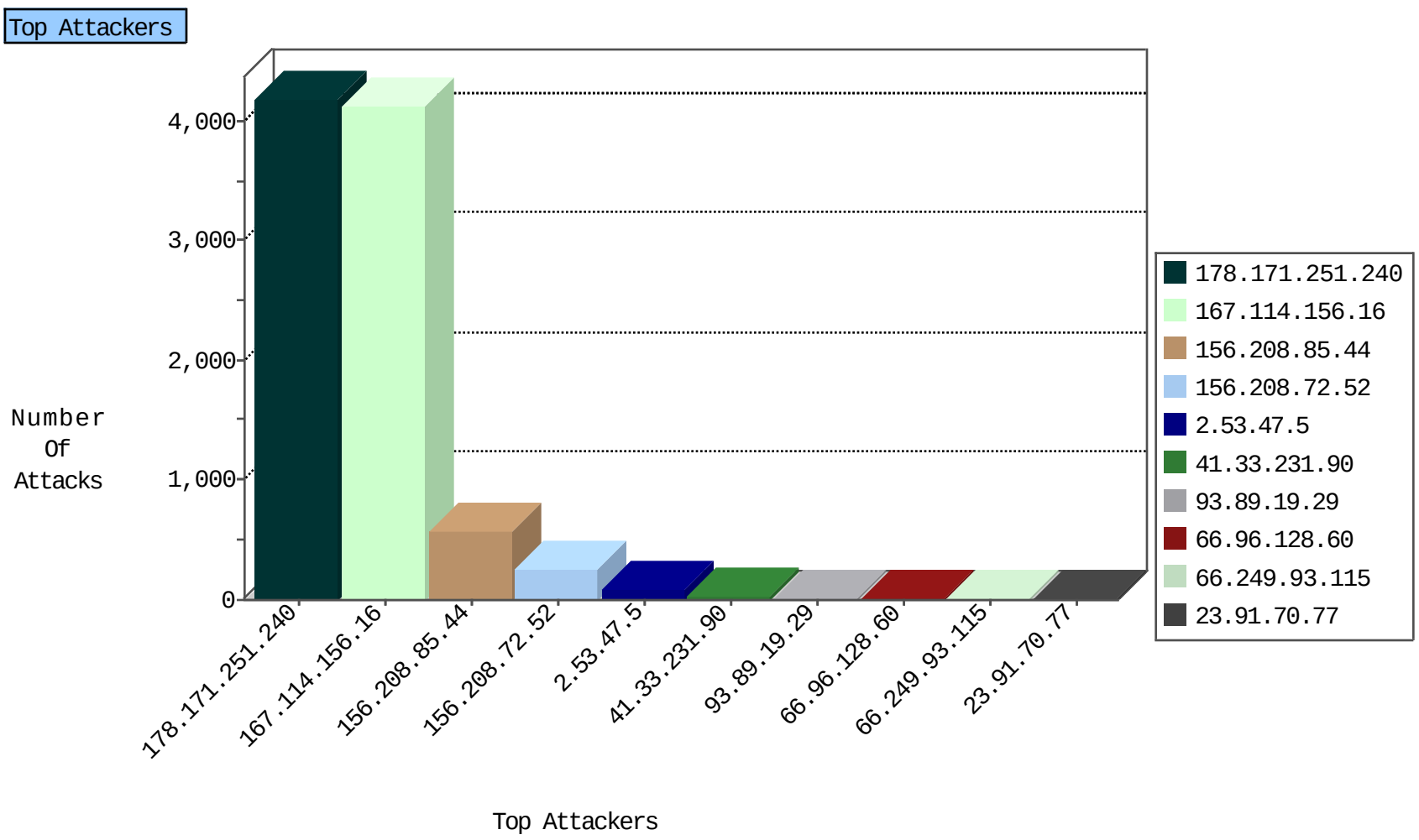
04-17-2016-04:04:06 to 04-17-2016-05:04:06

IDF Under Attack Daily Report





04-17-2016-04:04:06 to 04-17-2016-05:04:06

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	Block_Ip_Web_In	drop	4107
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	575
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	253
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	2
216.218.206.107	United States	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
179.43.141.194	Switzerland	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
179.43.141.194	Switzerland	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
179.43.141.194	Switzerland	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1

04-17-2016-04:04:06 to 04-17-2016-05:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.89.19.29	Turkey	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
93.89.19.29	Turkey	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
23.91.70.77	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
66.96.128.60	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
5.45.65.196	Netherlands	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-17-2016-04:04:06 to 04-17-2016-05:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.96.128.60	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	12
93.89.19.29	147.237.76.31	Turkey	nakchal.idf.il	SQL Injection - Select From	10
5.45.65.196	147.237.77.233	Netherlands	atal.idf.il	SQL Injection - Select From	6
23.91.70.77	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
70.89.127.78	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	3
97.74.4.26	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.142.238	147.237.76.34	France	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
212.129.33.79	147.237.76.199	France	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.92.47	147.237.76.39	Russian Federation	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
97.74.4.26	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.76.147		chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.113.67	147.237.8.50	Japan	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

04-17-2016-04:04:06 to 04-17-2016-05:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	3018
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	700
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	445
2.53.47.5	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	27
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.55.179.40	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack		reject	8
191.101.4.2	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
65.55.210.132	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.180.54.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
66.249.79.75	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.163	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.177.161.144	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
66.249.93.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.228.170.78	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
193.90.12.88	Norway	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
62.210.142.238	France	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
176.10.99.204	Switzerland	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
5.39.222.159	Netherlands	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.202	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.82	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.184.3.122	Japan	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.219	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.20.1.98	Turkey	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
123.126.113.80	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
199.87.154.251	Canada	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
89.35.178.104	Lithuania	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
65.19.167.130	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
176.10.99.209	Switzerland	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
5.199.130.188	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.203	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.90	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.184.3.122	Japan	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.251	United States	147.237.0.33	idf.il	drop		drop	1
74.82.47.12	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
62.210.142.238	France	147.237.0.16	my-kosher-kravi.idf.il	drop	First packet isn't SYN	drop	1
162.144.41.122	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.115.95.201	Anonymous Proxy	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
177.102.161.234	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.149.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.246	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

04-17-2016-04:04:06 to 04-17-2016-05:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.30.24.31	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
149.202.239.135	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	5
199.30.25.118	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
65.55.210.180	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.25.144	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
65.55.210.186	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
65.55.210.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
207.46.13.136	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.136	Block	2
79.180.54.103	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	2
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2349.jpg	Block	1
50.240.82.133	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/ãƒæ’ã†â€™ãƒâ€šã‚¢ãƒæ’ã‚¢ãƒâ€šã¬ã…â¡ãƒâ€šã‚¬ãƒæ’ã¢â€šã¬â¦ãƒâ€šã‚¯	Block	1
74.82.47.3	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/faq.aspx	Block	1
199.30.24.103	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/scripts.asmx/getjs	Block	1
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
65.55.210.128	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
198.58.103.158	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
12.252.239.222	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
149.202.239.135	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
68.180.230.115	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/1105-en/contactus.aspx	Block	1
199.30.16.165	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
37.77.135.30	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/chinuch.aspx	Block	1
157.55.39.32	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/templates/www.behazdaa.org.il	Block	1
68.180.230.184	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
199.30.16.182	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
105.155.26.188	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/recruitlane.aspx	Block	1
46.20.1.98	Turkey	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
203.157.127.18	Thailand	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
157.55.39.163	United States	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.163	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

04-17-2016-04:04:06 to 04-17-2016-05:04:06