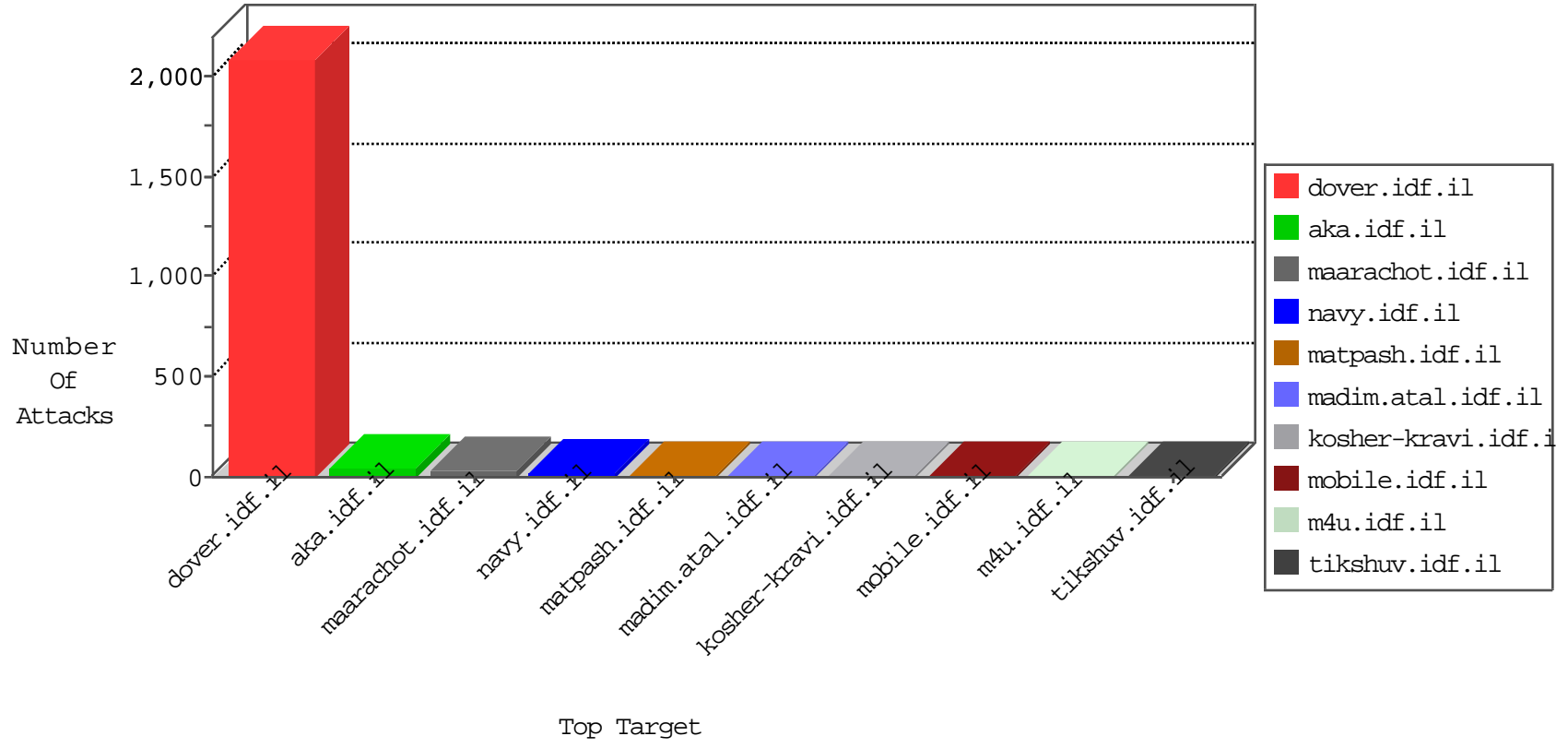


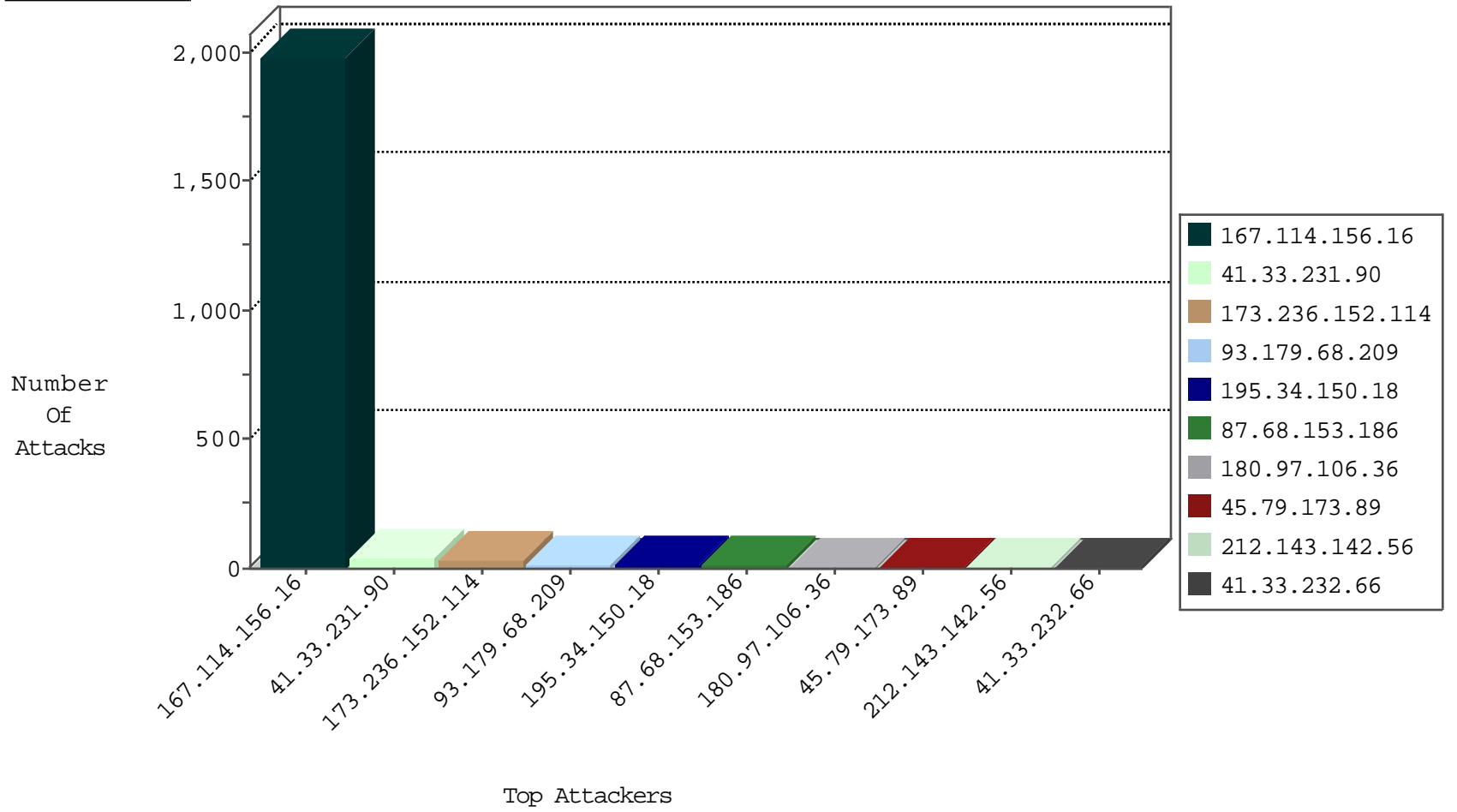
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3162
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	428
185.35.62.97	Switzerland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.89.35	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
66.176.172.168	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

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	5
173.236.152.114	147.237.77.170	United States	maarachot.idf.il	SERVER-WEBAPP backup access	5
66.249.78.2	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
201.172.121.42	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
196.203.149.99	147.237.0.19	Tunisia	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.108.132.58	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
196.203.149.99	147.237.0.19	Tunisia	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
196.203.149.99	147.237.0.19	Tunisia	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
186.182.101.198	147.237.8.28	Argentina	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
218.108.132.58	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1

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	36
87.68.153.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
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	5
45.79.173.89		147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
216.145.17.190	United States	147.237.77.176	matpash.idf.il	Header Rejection	header rejection pattern found in request	monitor	4
66.249.69.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.109.3.6	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
40.77.167.7	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
40.77.167.39	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
68.65.120.48		147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
61.135.190.200	China	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	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
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.163.68.111	Germany	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.167	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
87.69.87.39	Israel	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
45.79.173.89		147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	2
54.80.6.9	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.117	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.111	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
139.196.104.39	China	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.75	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.37	China	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	1
141.212.122.212	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.154.146.225	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
46.19.86.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.96	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.107	United States	147.237.0.35	akaws.idf.il	drop		drop	1
109.186.31.223	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.162	China	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
180.97.106.36	China	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
216.218.206.114	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.118	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.200	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.68	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.96	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
180.97.106.37	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
141.212.122.99	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.107	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.186.31.223	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.97.106.162	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
69.122.148.186	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.36	China	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1
216.218.206.122	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
63.229.211.34	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.236.152.114	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 173.236.152.114	Block	14
173.236.152.114	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	10
93.179.68.209	United Kingdom	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
93.179.68.209	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.179.68.209	Block	5
84.228.35.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
207.46.13.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/error.htm	Block	2
46.19.85.219	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/patzar/Klali/default.asp	None	1
46.19.85.219	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
203.215.121.213	Philippines	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
173.180.255.19	Canada	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19412-he/idfgdover.aspx	Block	1
182.96.106.195	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.117.164.60	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19916-he/idfgdover.aspx	Block	1
184.105.139.67	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
40.77.167.39	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/kamlar/contact/	None	1
131.253.25.154	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/i/jot	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
46.117.164.60	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.117.164.60	None	1
173.236.152.114	United States	147.237.77.170	maarachot.idf.il	Multiple Admin Blocking from 173.236.152.114	Block	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/62312	Block	1
40.77.167.45	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
184.105.139.68	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
157.55.39.194	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/x³xÿ	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
46.163.68.111	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
207.46.13.145	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.179.68.209	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
203.215.121.213	Philippines	147.237.77.74	law.idf.il	PHP Attempt	Block	1
173.180.255.19	Canada	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
61.135.190.197	China	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on 147.237.0.19/	Block	1
176.12.139.113	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1