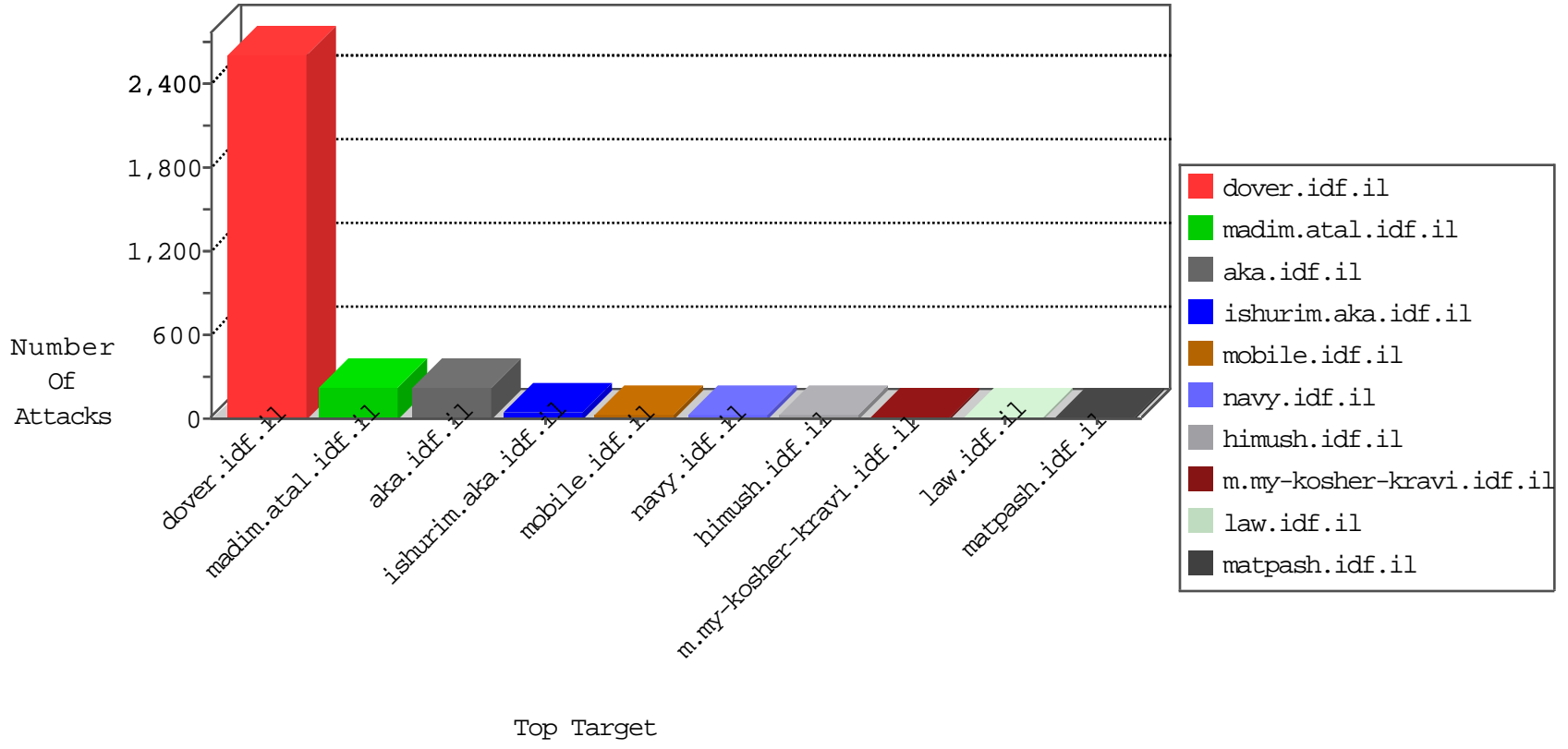


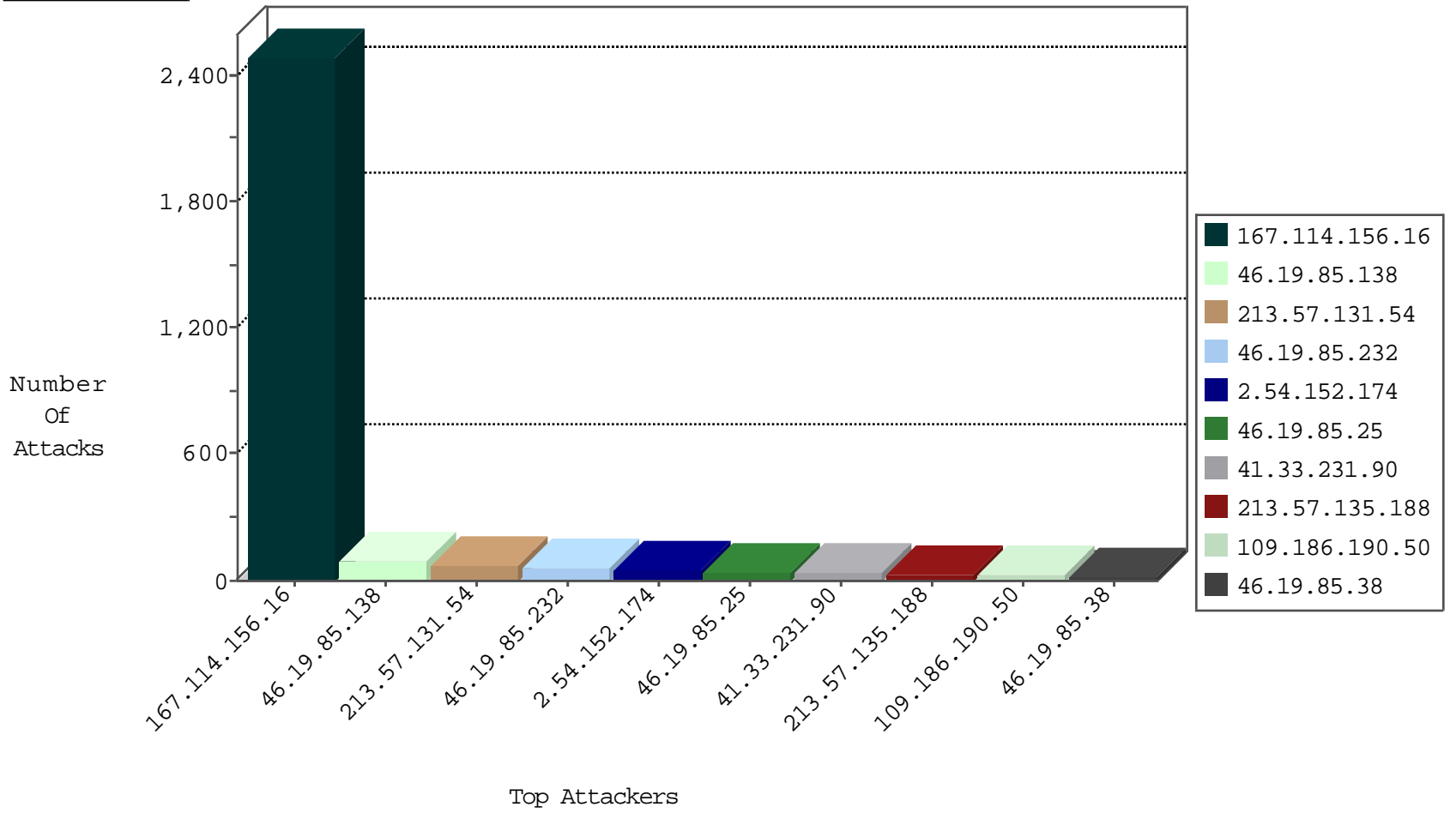
IDF Under Attack Daily Report



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	3419
134.147.203.115	Germany	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
118.193.23.46	China	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
183.89.123.35	Thailand	147.237.76.201	e.atal.idf.il	JIM_Purple_Con_Limit_Http	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
94.75.220.155	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
94.75.220.155	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
109.67.146.72	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.19.178.10	147.237.77.216	Germany	dover.idf.il	Tehila - Perl LWP with fake user agent	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
85.236.191.80	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
62.38.250.31	147.237.77.205	Greece	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
31.211.102.129	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN NMAP -sS window 4096	1
191.33.46.223	147.237.77.179	Brazil	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
166.63.125.149	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
94.75.220.155	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
85.236.191.80	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
85.236.191.80	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
85.236.191.80	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
62.38.250.31	147.237.77.205	Greece	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
212.179.177.148	147.237.72.167	Israel	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
62.38.250.31	147.237.77.205	Greece	prisha.idf.il	ET SCAN NMAP -f -sS	1
191.33.46.223	147.237.77.179	Brazil	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
191.33.46.223	147.237.77.179	Brazil	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
166.63.125.149	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
94.75.220.155	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
85.236.191.80	147.237.0.33	Russian Federation	idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.25	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
213.57.131.54	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	33
213.57.131.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	33
109.64.235.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.186.190.50	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.38	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.57.135.188	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
213.57.135.188	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
213.57.135.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
109.186.190.50	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
149.78.207.50	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
37.26.149.174	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
128.78.78.156	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.152.174	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.202.238	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.120.23.125	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.173.197	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.142.150.172	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.186.190.50	Israel	147.237.76.30	himush.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.185.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.111.191.57	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.181.99.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.12.137.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.188	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.232	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.185.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.109.10.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
95.108.158.194	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
89.138.230.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.178.96.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.22.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.19.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.142.150.172	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
89.138.230.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.86.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
207.46.13.139	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.10	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.48	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
188.120.148.181	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
2.54.152.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.54.152.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
37.142.64.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
5.28.131.167	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.28.131.167	Block	7
46.120.46.55	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
179.43.138.165	Switzerland	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/homepage/	Block	4
168.235.196.240	United States	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	4
31.154.167.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.29.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.19.178.10	Germany	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
149.88.4.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
168.235.196.240	United States	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	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
84.19.178.10	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.19.178.10	Block	2
141.212.122.112	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to /x	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/8/4538.pdf	Block	1
109.64.235.248	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.29.43.182	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
89.138.54.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/wassachhh	Block	1
79.178.135.128	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.137.201	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
109.160.179.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: 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
37.140.141.38	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
73.254.96.42	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.120.46.55	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPersonalId in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	1
109.64.235.248	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
5.29.43.182	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
207.46.13.139	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/navmenu/	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
79.179.150.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.63.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.142.251	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
141.8.142.1	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1361-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
5.28.131.167	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
185.3.146.85	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ctl100\$cpMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
84.19.178.10	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19069-en/dover.aspx&	Block	1
150.70.188.169	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
77.126.26.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
52.90.226.14	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/163	Block	1
109.65.96.254	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
31.13.110.121	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
94.194.56.144	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1