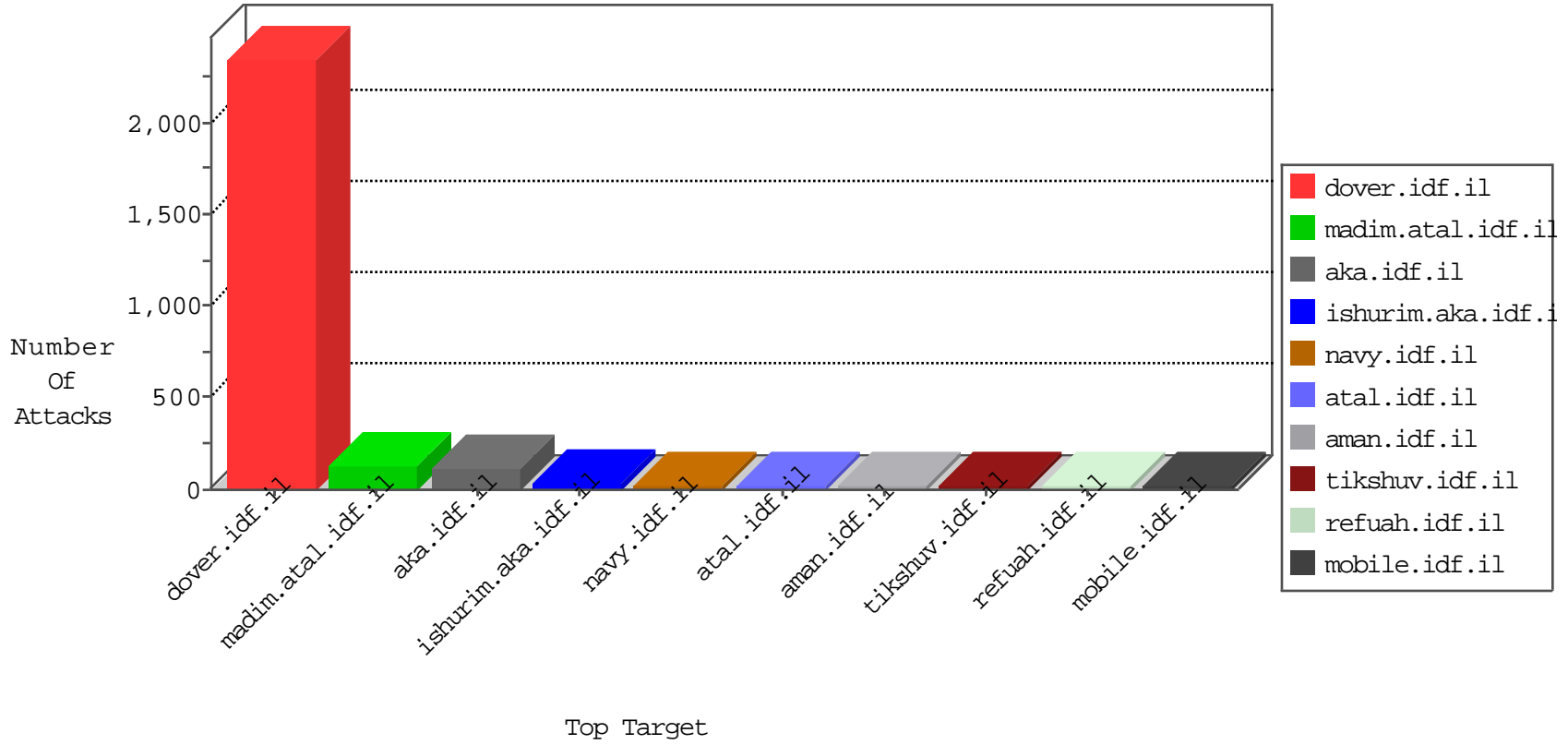


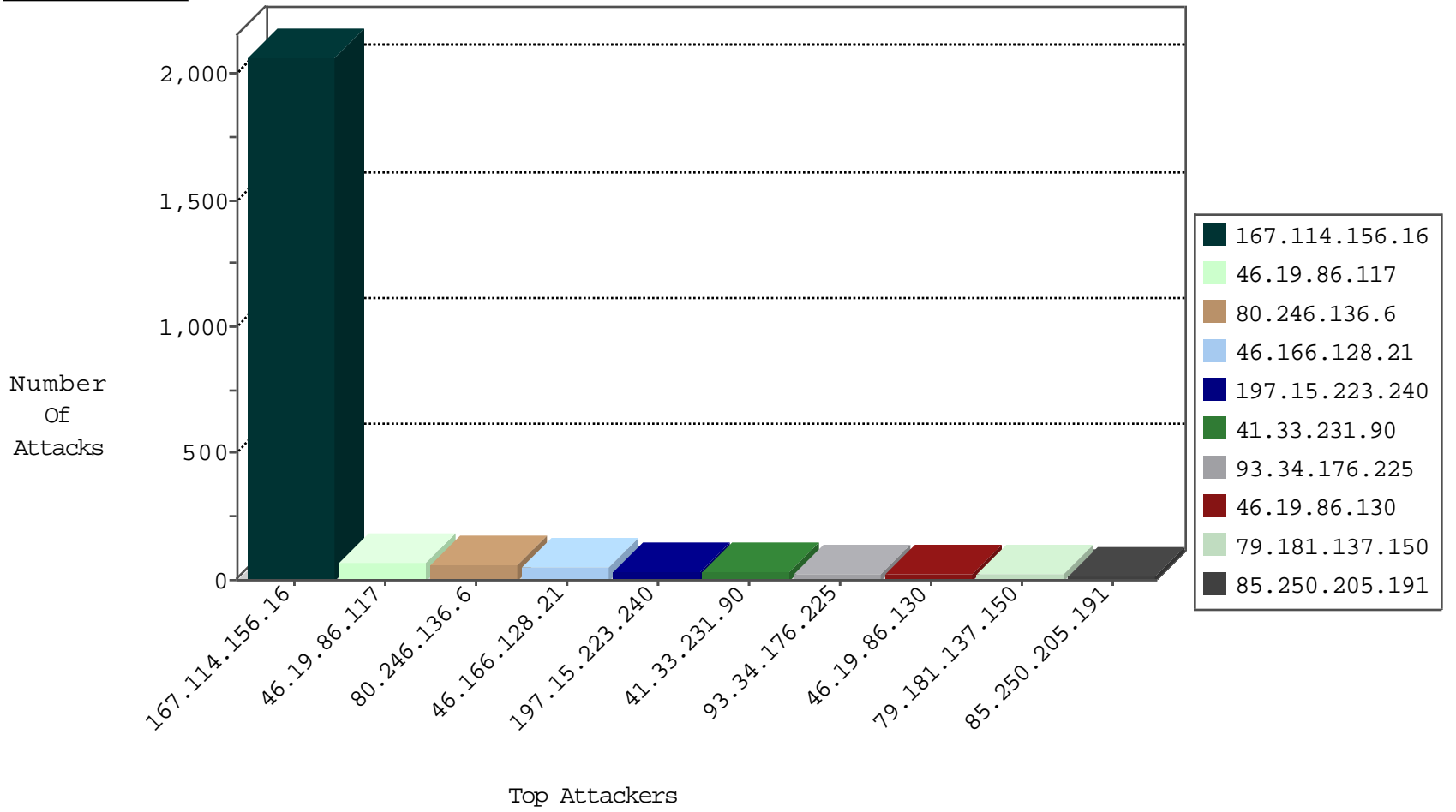
IDF Under Attack Daily Report



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	3078
115.239.228.10	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
119.229.247.152	Japan	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
71.6.158.166	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
99.236.101.63	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.197.177.26	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
151.80.31.118	Italy	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	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	4
66.249.78.69	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
118.163.199.147	147.237.76.38	Taiwan	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.77.226	Canada	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
197.15.223.240	147.237.76.42	Tunisia	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.167.162	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
197.15.223.240	147.237.76.42	Tunisia	refuah.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.162	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
197.15.223.240	147.237.76.31	Tunisia	nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
118.163.199.147	147.237.76.38	Taiwan	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
114.215.111.222	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.162	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
197.15.223.240	147.237.76.42	Tunisia	refuah.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
89.248.167.162	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
197.15.223.240	147.237.76.31	Tunisia	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.167.162	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
197.15.223.240	147.237.76.30	Tunisia	himush.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
164.39.11.198	147.237.76.34	United Kingdom	yohalan.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	30
46.19.86.130	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
79.181.137.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
85.250.205.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
37.26.146.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
84.111.226.232	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
46.166.128.21	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
80.178.198.56	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
176.13.3.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.64.122.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.250.61.112	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
176.13.3.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
37.26.148.163	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.166.128.21	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	8
46.166.128.21	Netherlands	147.237.77.216	dover.idf.il	SYN Attack		reject	8
197.15.223.240	Tunisia	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.49	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
89.138.91.229	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
93.34.176.225	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.166.128.21	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.147.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.34.176.225	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.166.128.21	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.3.144.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.138.91.229	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
197.15.223.240	Tunisia	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
134.61.71.222	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
134.61.71.222	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
5.22.131.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
93.34.176.225	Italy	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
185.3.144.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.60	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
109.65.154.117	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.166.128.21	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
207.46.13.10	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.250.205.191	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	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
93.34.176.225	Italy	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
93.34.176.225	Italy	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.166.128.21	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.128.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.204.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.30.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
80.246.136.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
46.19.86.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
2.54.27.182	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/1133-22638-he/dover.aspx.	Block	2
91.109.247.173	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
141.212.122.145	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	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
77.125.6.197	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
5.144.55.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.201.152.236	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
95.86.69.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
188.120.148.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
213.57.108.16	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
37.26.147.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.136.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.218.241.125	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
46.19.86.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.104.235	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.108.168.159	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mazi.idf.il	Block	1
46.19.86.17	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.aspx/search	Block	1
104.131.147.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	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
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	1
46.166.186.198	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
2.54.132.116	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.161.153	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.65.161.153	Block	1
85.64.71.45	Israel	147.237.72.166	aka.idf.il	Too Many Cookies in a Request - 104 cookies	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1400-he/atal.aspx	Block	1
141.212.122.145	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
46.19.86.74	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	1
66.249.64.17	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/navmenu/	Block	1
2.54.145.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.161.153	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/milluim/index	Block	1