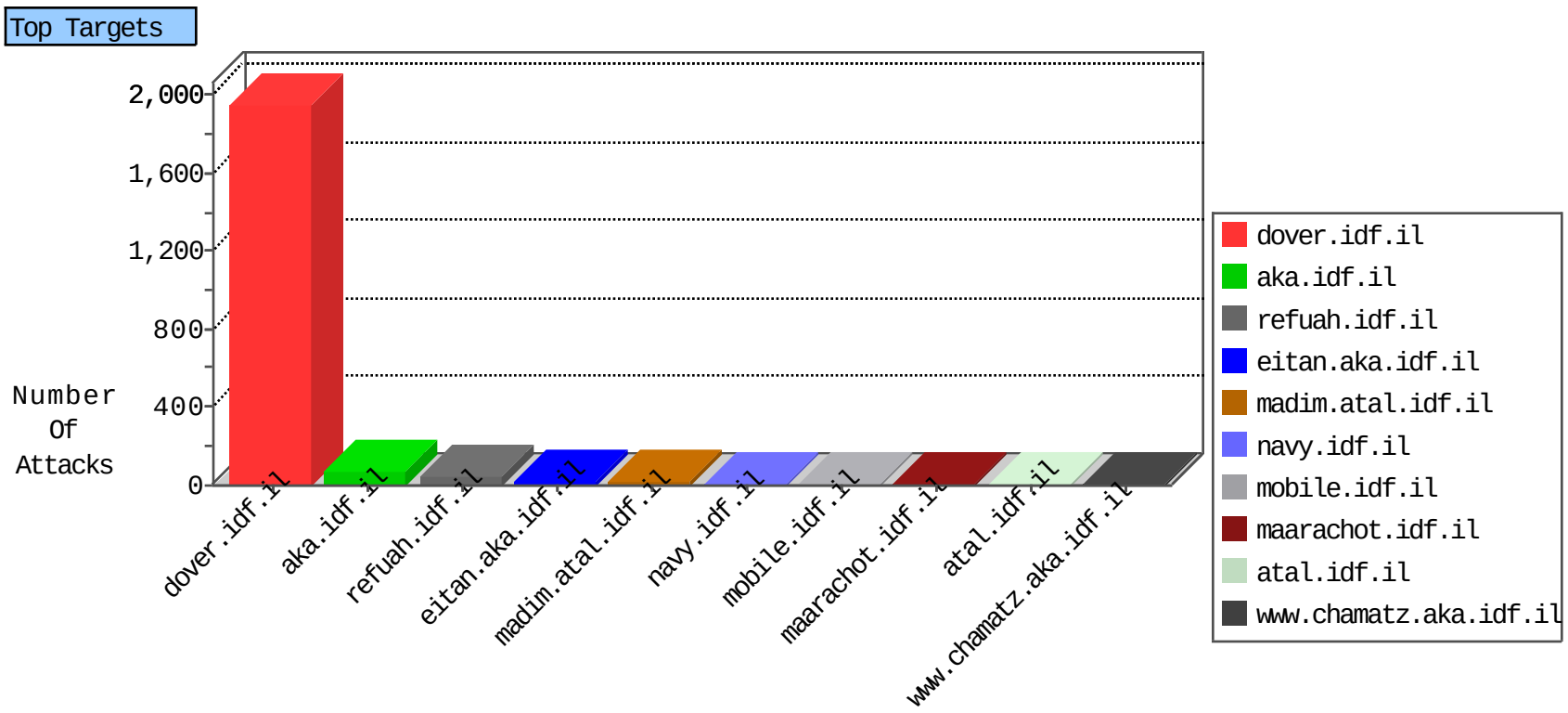
01-08-2016-01:07:30 to 01-08-2016-02:07:30

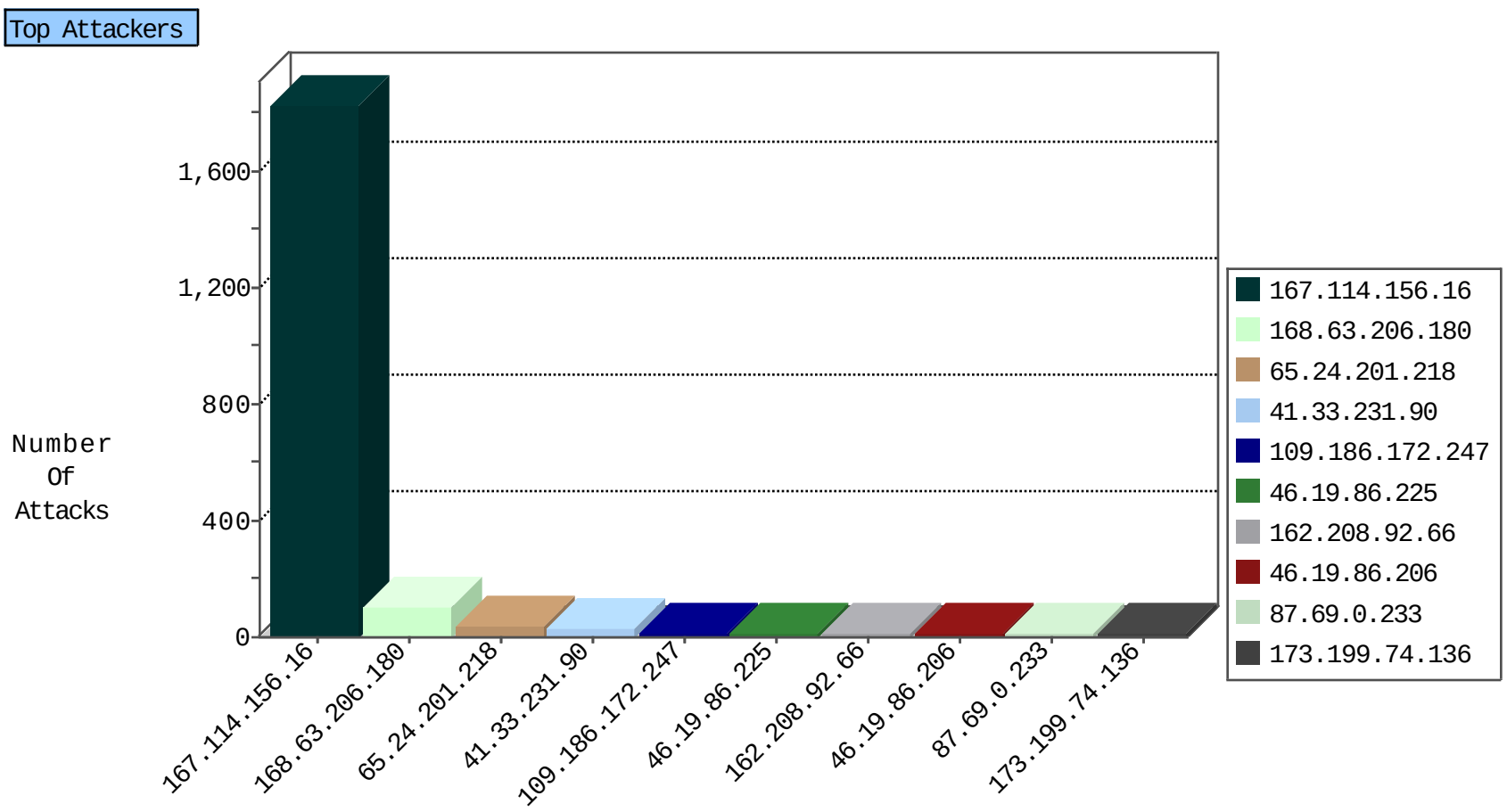
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-08-2016-01:07:30 to 01-08-2016-02:07:30

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	3158
66.249.73.238	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	36
218.95.228.109	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
218.95.228.109	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

01-08-2016-01:07:30 to 01-08-2016-02:07:30

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-08-2016-01:07:30 to 01-08-2016-02:07:30

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
168.63.206.180	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
168.63.206.180	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
168.63.206.180	147.237.76.86	United States	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
168.63.206.180	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
168.63.206.180	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
168.63.206.180	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
168.63.206.180	147.237.77.170	United States	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
168.63.206.180	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
168.63.206.180	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
168.63.206.180	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
168.63.206.180	147.237.0.33	United States	idf.il	ET SCAN Potential VNC Scan 5900-5920	3
168.63.206.180	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
168.63.206.180	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
168.63.206.180	147.237.77.234	United States	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
168.63.206.180	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
168.63.206.180	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	147.237.77.212	United States	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
173.199.74.136	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	147.237.72.166	United States	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
173.199.74.136	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
115.182.249.11	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
115.182.249.11	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
168.63.206.180	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
168.63.206.180	147.237.77.74	United States	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
168.63.206.180	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
83.99.63.1	147.237.77.216	Luxembourg	dover.idf.il	ET SCAN NMAP -sS window 4096	1
168.63.206.180	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
168.63.206.180	147.237.76.30	United States	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.8.46	United Kingdom	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
77.127.187.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.63.206.180	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
168.63.206.180	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
168.63.206.180	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
168.63.206.180	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
121.12.173.62	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1

01-08-2016-01:07:30 to 01-08-2016-02:07:30

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
65.24.201.218	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
109.186.172.247	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
162.208.92.66	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
46.19.86.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
87.69.0.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.181	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.206	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.11.255	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.55.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.95	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.130.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
85.64.181.132	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
149.78.252.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.240	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.125.148.86	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.76.127.111	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
5.29.206.9	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
67.232.142.136	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
61.135.190.72	China	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
188.143.232.10	Russian Federation	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
188.143.232.10	Russian Federation	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
62.0.200.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
81.44.224.176	Spain	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
185.106.92.33		147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.117.232.161	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.98	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.83	United States	147.237.0.33	idf.il	drop		drop	1
87.69.245.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
149.88.226.249	Israel	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.85	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.65.104.196	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.106.92.33		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
51.255.224.217	United Kingdom	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.19.85.236	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.84	United States	147.237.0.33	idf.il	drop		drop	1
87.69.245.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.93	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
218.22.211.69	China	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
85.130.247.49	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

01-08-2016-01:07:30 to 01-08-2016-02:07:30

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.164.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.253.201.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
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
46.19.86.119	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
84.229.150.233	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/size220x0/sip_storage	Block	2
37.26.146.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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
65.24.201.218	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method Â¬[[#0]][[#0]][[#0]]AÂ¢	Block	1
40.77.167.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 40.77.167.42	Block	1
79.177.133.63	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 79.177.133.63	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-14885-he/dover.aspx	Block	1
185.106.92.33		147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
2.54.170.248	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	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
68.180.229.62	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
65.24.201.218	United States	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
40.77.167.42	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
109.253.212.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.11.255	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19926-he/dover.aspx	Block	1
188.143.232.10	Russian Federation	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 188.143.232.10	Block	1
46.166.186.196	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
5.29.206.9	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1035-ar/cogat.aspx	Block	1
65.24.201.218	United States	147.237.76.42	refuah.idf.il	NULL Character in Method Â¬[[#0]][[#0]][[#0]]AÂ¢	Block	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
114.98.226.56	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1356-he/cogat.aspx/trackback/	Block	1
40.77.167.95	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.152.16	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 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
188.143.232.10	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/faq/faq.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
65.24.201.218	United States	147.237.76.42	refuah.idf.il	Abnormally Long Header Line request header name	Block	1
109.64.7.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.244.254.229	Austria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
65.24.201.218	United States	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/	Block	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/_api/getdiarycalendar.php	Block	1
141.212.122.64	United States	147.237.77.74	law.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
46.19.85.97	Israel	147.237.76.39	mobile.meitav.idf.il	Multiple Untraceable SSL Sessions from 46.19.85.97 (Open Mode)	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
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf/templates/innerpage.aspx	Block	1
65.24.201.218	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Header Name	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.72.238.241	Block	1
109.67.9.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.41.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
65.24.201.218	United States	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method Â¬[[#0]][[#0]][[#0]]AÂ¢ in URL	Block	1
213.57.236.190	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1

01-08-2016-01:07:30 to 01-08-2016-02:07:30