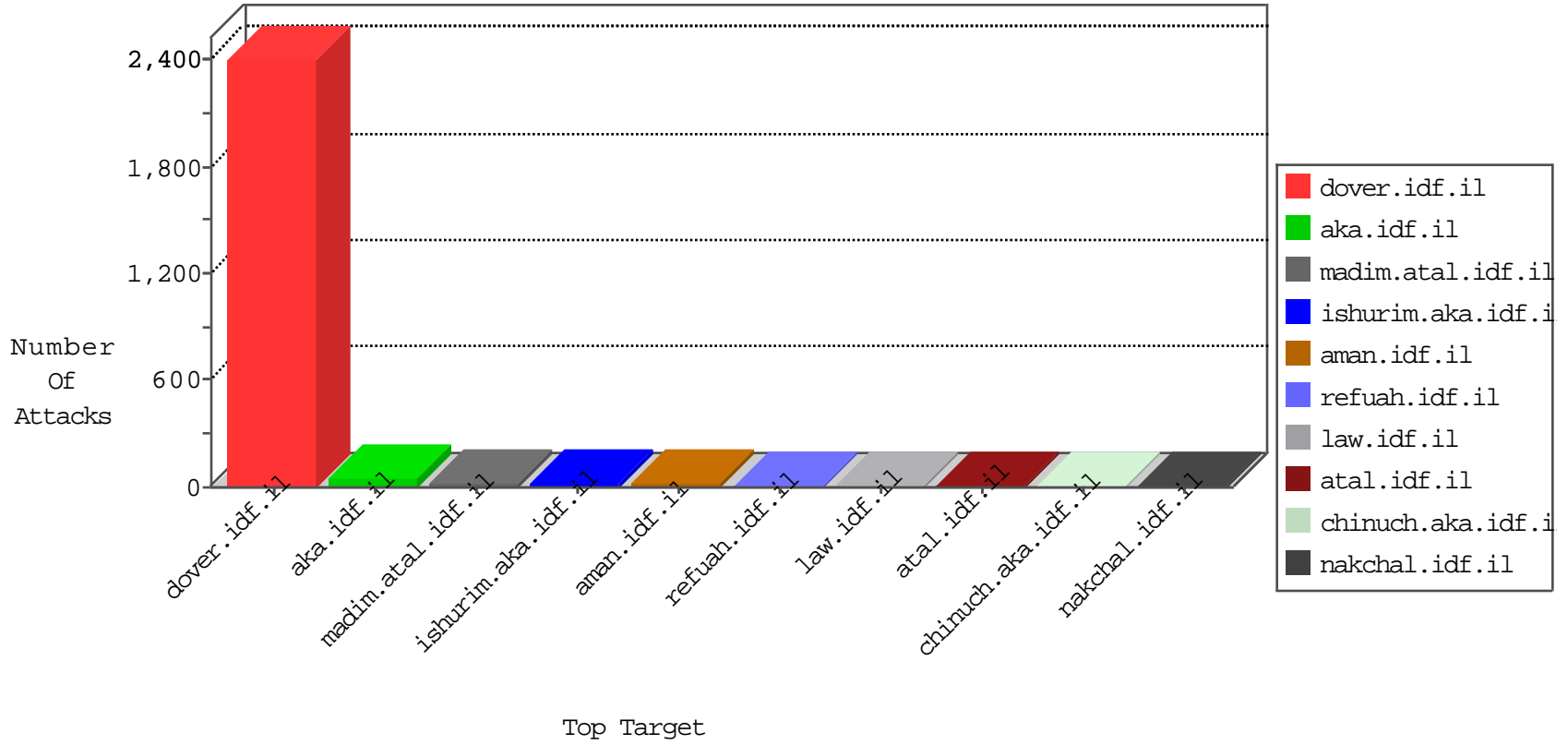


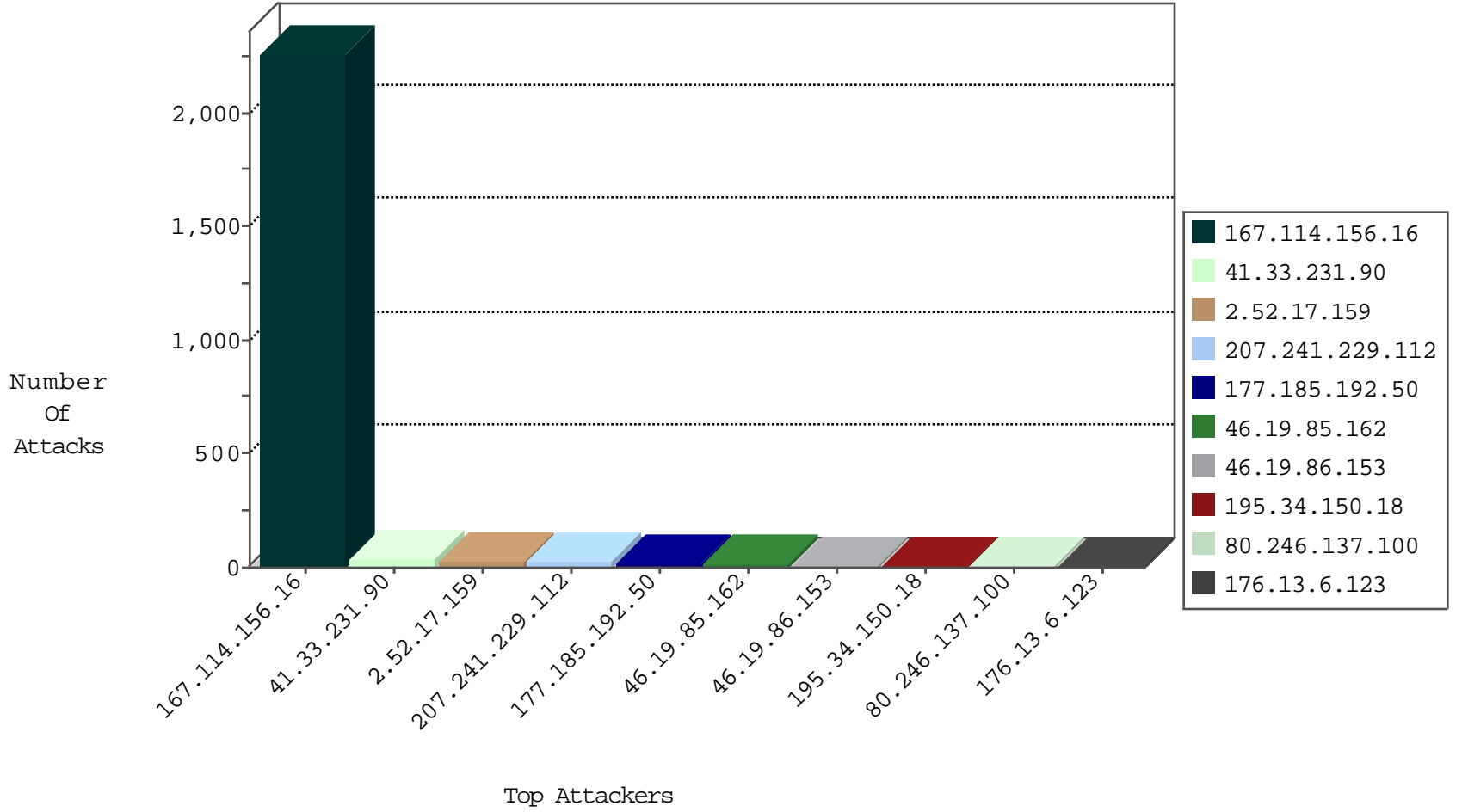
# IDF Under Attack Daily Report



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	3561
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1215

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.22.47.242	Finland	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
177.185.194.45	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
5.9.111.70	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
93.89.16.110	Turkey	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	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
177.185.194.45	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	3
66.249.64.191	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
209.126.230.71	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential SSH Scan	1
209.126.230.71	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
196.12.190.13	147.237.77.227	Puerto Rico	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
193.105.134.220	147.237.76.44	Sweden	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
113.106.129.219	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
52.6.202.63	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -f -sS	1
209.126.230.71	147.237.77.243	United States	mobile.idf.il	ET SCAN Potential SSH Scan	1
209.126.230.71	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
209.126.230.71	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
93.89.16.110	147.237.72.166	Turkey	aka.idf.il	SQL Injection - Select From	1
52.6.202.63	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 2048	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
207.241.229.112	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
177.185.192.50	Brazil	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
2.52.17.159	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.52.17.159	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
207.241.229.112	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
130.15.34.11	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.164.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.52.17.159	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.117.225.202	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.52.17.159	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
46.19.86.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
66.249.78.2	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.88.26.114	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.164.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
177.185.192.50	Brazil	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	2
40.77.167.89	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.133	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
195.154.227.118	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
46.19.86.29	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
123.126.113.80	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
46.19.86.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.82	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
155.94.222.12	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
87.68.46.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
65.254.225.176	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
193.105.134.220	Sweden	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.29	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.24	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.153	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.95	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
155.94.222.12	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
89.247.20.73	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.240.236.119	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
193.105.134.220	Sweden	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
46.19.86.29	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.31	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.72	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.6.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.246.137.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
166.170.34.66	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
79.179.136.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.202	United States	147.237.76.147	chinuch.aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	2
46.117.181.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
82.81.25.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	2
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	2
46.19.85.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
85.136.227.77	Spain	147.237.72.166	aka.idf.il	Multiple signatures from 85.136.227.77	Block	1
66.249.78.20	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakchal.aspx	Block	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	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
177.185.192.50	Brazil	147.237.72.156	aman.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	1
89.138.97.187	Israel	147.237.72.166	aka.idf.il	Unknown Parameter _ in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.78.27	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/2/1682.doc	Block	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
177.185.192.50	Brazil	147.237.72.156	aman.idf.il	Multiple signatures from 177.185.192.50	Block	1
98.19.222.133	United States	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter cat.. in www.aka.idf.il/chinuch/home/default.asp	None	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
207.46.13.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16552-en/dover.aspx-title=for	Block	1
157.55.39.230	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.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
98.19.222.133	United States	147.237.72.166	aka.idf.il	Multiple signatures from 98.19.222.133	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
40.77.167.89	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/css/combinestyleshandler.ashx	Block	1
85.136.227.77	Spain	147.237.72.166	aka.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
79.178.122.211	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1