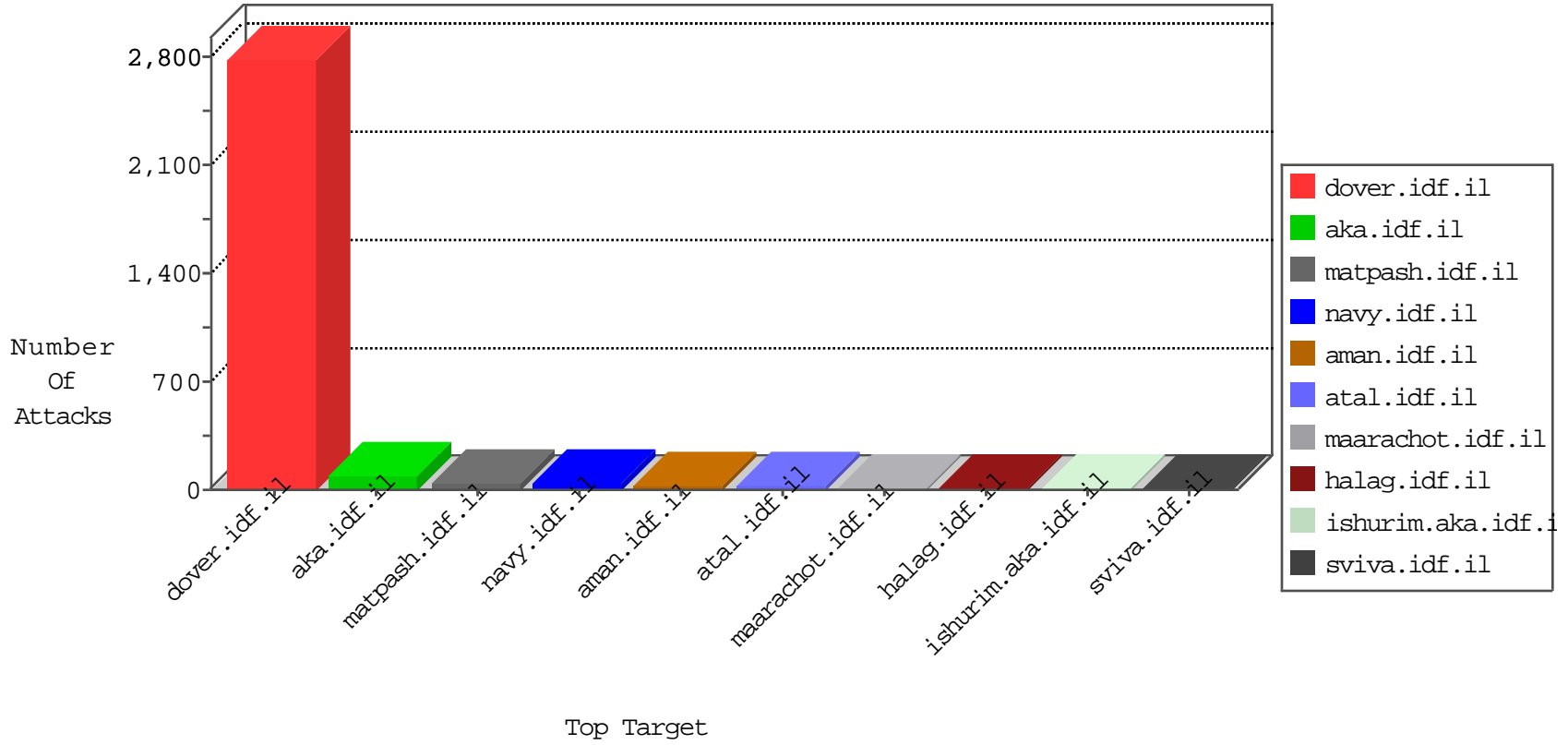


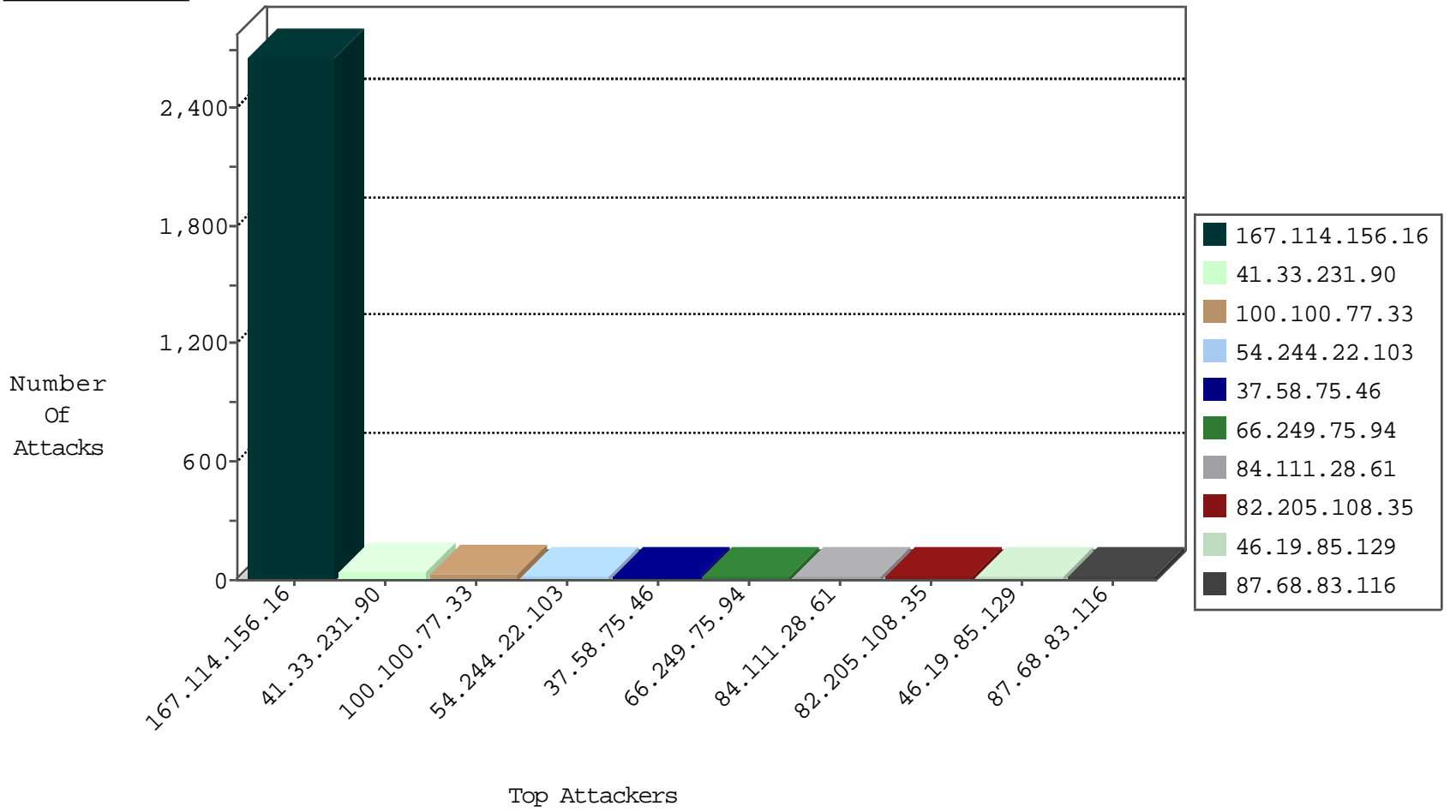
IDF Under Attack Daily Report



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	3408
183.60.48.25	China	147.237.76.34	yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.58.75.46	Netherlands	147.237.77.235	sviva.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
37.58.75.46	Netherlands	147.237.77.233	atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
37.58.75.46	Netherlands	147.237.77.234	halag.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
185.106.94.2		147.237.76.39	mobile.meitav.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	2
185.106.94.2		147.237.76.86	navy.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1
37.58.75.46	Netherlands	147.237.77.235	sviva.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
37.58.75.46	Netherlands	147.237.77.233	atal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
37.58.75.46	Netherlands	147.237.77.234	halag.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	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
24.37.76.186	147.237.77.233	Canada	atal.idf.il	ET SCAN NMAP -sS window 4096	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
122.96.31.37	147.237.77.170	China	maarachot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.195	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
37.58.75.46	147.237.77.234	Netherlands	halag.idf.il	ET WEB_SERVER Muieblackcat scanner	1
31.6.71.154	147.237.77.170	Poland	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.107	147.237.76.34	China	yochalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
176.13.18.141	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
109.235.254.181	147.237.76.201	Turkey	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
37.58.75.46	147.237.77.235	Netherlands	sviva.idf.il	ET WEB_SERVER Muieblackcat scanner	1
37.58.75.46	147.237.77.233	Netherlands	atal.idf.il	ET WEB_SERVER Muieblackcat scanner	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
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	22
66.249.75.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
82.205.108.35	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
79.178.141.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.236.24.54	United Kingdom	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.197	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
84.111.28.61	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
176.13.18.141	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.180.53.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.90.167.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.186.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.161.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
78.98.38.148	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.111.28.61	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
80.178.13.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.185	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.69.65.40	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.201.138.16	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.178.200.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.65.40	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.102.247.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.18.141	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
149.78.22.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.211.194	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
62.210.206.219	France	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
87.68.83.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
66.249.75.102	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.54.186.32	Israel	147.237.72.166	aka.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
87.68.83.116	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
208.115.111.73	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
141.212.121.221	United States	147.237.76.198	e.yochalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
149.78.201.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.117.38.55	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
42.62.74.76	China	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
64.125.239.36	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.121.222	United States	147.237.76.198	e.yochalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
31.168.13.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
213.8.174.6	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
157.55.39.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
31.210.186.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	5
103.9.64.130	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
207.46.13.119	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.119	Block	3
184.154.14.15	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
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	2
103.9.64.130	Australia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
5.29.76.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
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	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
184.154.14.15	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
46.19.86.53	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.142.68.40	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
184.154.14.15	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
37.142.68.40	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	2
37.142.68.59	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	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
84.111.28.61	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyius/kadatz	Block	1
197.35.117.192	Egypt	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
149.78.82.159	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.19.86.33	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
207.46.13.119	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
79.177.198.21	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
184.154.14.15	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 184.154.14.15	Block	1
37.142.68.59	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/xmlrpc.php	Block	1
84.111.202.66	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$questionUpdate\$hiddenUpdateQuest ion in www.aka.idf.il/main/gyius/faq.aspx	None	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration/government/pages/tikshoret1.aspx	Block	1
197.35.117.192	Egypt	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
157.55.39.64	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
46.19.86.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/ishurim/cityofficers/	None	1
79.178.55.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
40.77.167.21	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/1/1381.pdf	Block	1
109.65.207.237	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
85.65.116.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.76.106.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$employmentStatusDay in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	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
103.9.64.130	Australia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 103.9.64.130	Block	1
208.115.113.89	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
79.183.179.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
185.32.179.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.207.237	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct179 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
85.65.236.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.107.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1