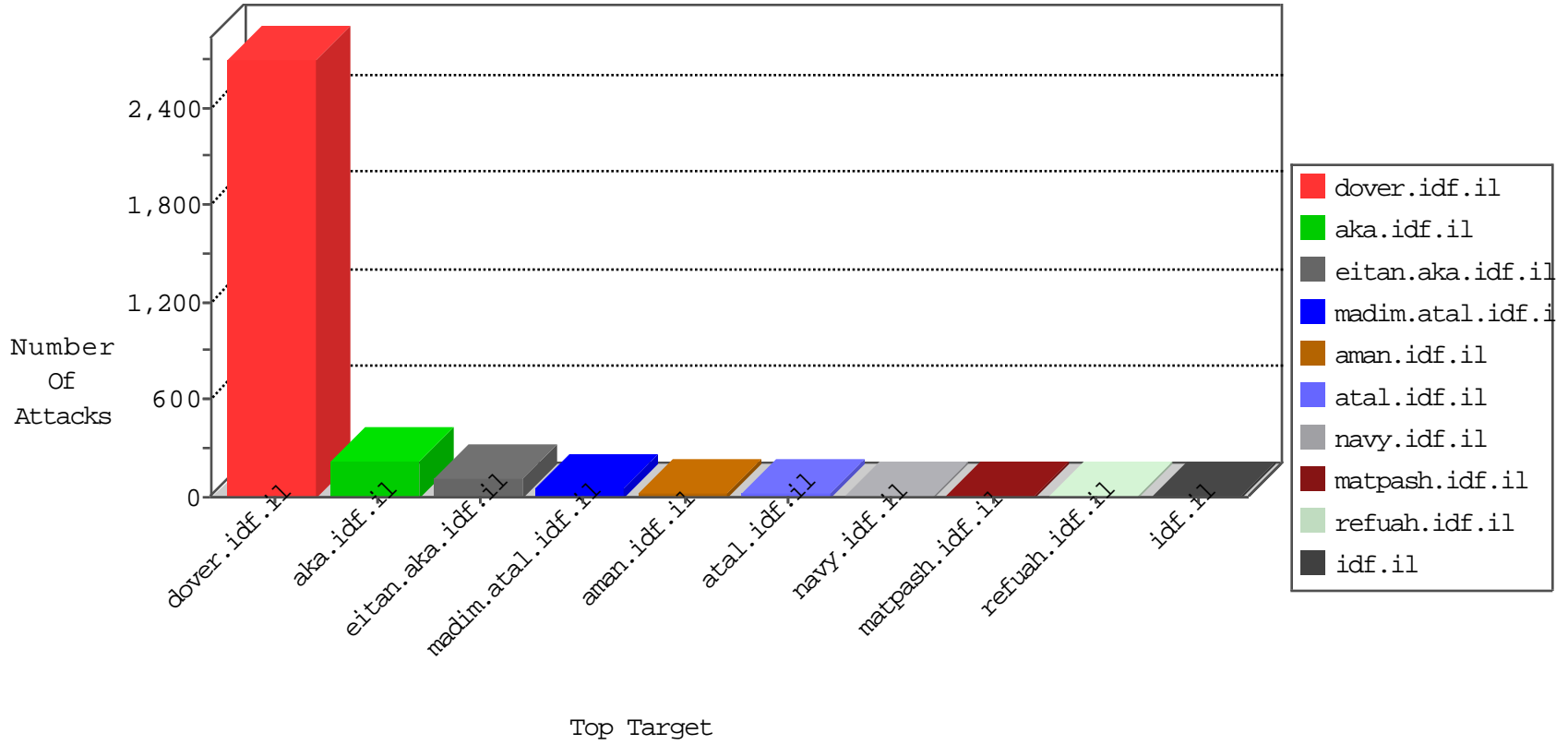


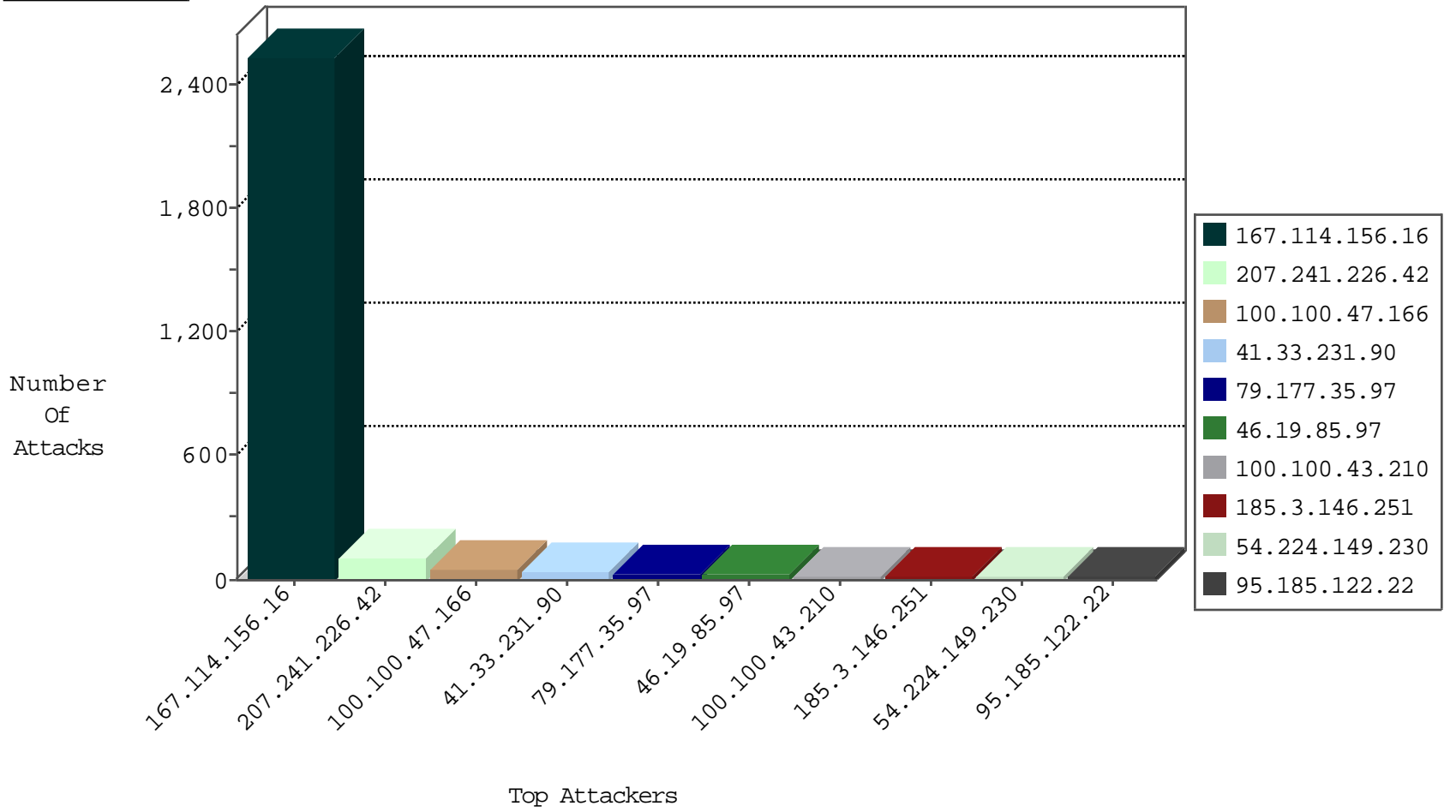
IDF Under Attack Daily Report



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	3543
75.104.23.170	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	5
115.231.222.40	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Http	drop	2
112.218.14.140	Korea, Republic of	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
167.114.229.245	Canada	147.237.77.176	matpash.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
195.154.188.28	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.191.213	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
54.224.149.230	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	13
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
85.165.60.202	147.237.0.33	Norway	idf.il	ET SCAN Potential SSH Scan	3
66.249.66.78	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.246	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
105.186.194.35	147.237.0.17	South Africa	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
195.154.191.213	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	1
85.165.60.202	147.237.76.42	Norway	refuah.idf.il	ET SCAN Potential SSH Scan	1
195.154.191.213	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS) .asp Filename Extension Parsing File Upload Security Bypass Attempt (asp)	1
190.213.165.102	147.237.8.50	Trinidad and Tobago	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
85.165.60.202	147.237.0.15	Norway	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
190.213.165.102	147.237.8.24	Trinidad and Tobago	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
79.174.70.237	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
190.213.165.102	147.237.0.34	Trinidad and Tobago	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
190.213.165.102	147.237.0.19	Trinidad and Tobago	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
158.255.29.101	147.237.8.24	Slovakia	e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
36.232.151.11	147.237.0.17	Taiwan	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
209.126.116.147	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
105.186.194.35	147.237.0.33	South Africa	idf.il	ET SCAN Potential SSH Scan	1
201.235.198.226	147.237.76.31	Argentina	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
85.165.60.202	147.237.76.86	Norway	navy.idf.il	ET SCAN Potential SSH Scan	1
195.154.191.213	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	1
85.165.60.202	147.237.0.34	Norway	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
85.165.60.202	147.237.0.16	Norway	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
190.213.165.102	147.237.8.28	Trinidad and Tobago	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
79.174.70.237	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN Potential SSH Scan	1
190.213.165.102	147.237.0.35	Trinidad and Tobago	akaws.idf.il	ET SCAN Potential SSH Scan	1
190.213.165.102	147.237.0.33	Trinidad and Tobago	idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
190.213.165.102	147.237.0.16	Trinidad and Tobago	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
51.254.46.129	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
119.247.254.196	147.237.76.31	Hong Kong	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
209.126.116.147	147.237.0.16	United States	my-kosher-kravi.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
100.100.47.166		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
100.100.43.210		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
95.185.122.22	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
46.19.85.131	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
100.100.28.123		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
80.246.137.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
77.125.90.196	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.53.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.182.0.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.106.227.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
213.57.44.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
94.230.86.190	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
207.46.13.81	United States	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
5.29.47.102	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.64.164.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.40.47.82	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
77.125.74.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.174.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.38.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.177.99.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.107.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.34		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.109	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
100.100.70.255		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
5.29.233.119	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
100.100.118.74		147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
185.3.144.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.46.39.101	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
84.109.232.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.52.146.23	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
208.115.111.73	United States	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.160.173.218	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.23	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.241.226.42	United States	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 207.241.226.42	Block	97
79.177.35.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
185.3.146.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
79.177.223.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
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
85.65.71.43	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.12.143.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.67.138	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
54.224.149.230	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/usercontrols/headerupper/	Block	1
2.54.2.233	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
77.125.4.74	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
66.249.66.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	1
149.78.43.170	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.85.131	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
79.183.107.232	Israel	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	1
212.76.102.15	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/3/3373.pdf&sa=u&ved=0ahukewiao-zf1bvjahwb7xqkhebjdqwqfeggvmau&usg=afqjcnf3_xtjyib6met3xcdmg53pdv7jq	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
195.154.168.82	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
2.54.19.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.207.174	Israel	147.237.0.16	my-kosher-kravi.idf.il	Parameter Type Violation Master\$ContentPlaceHolder1\$password in my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
79.176.19.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.241.226.42	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/a	Block	1
173.252.74.104	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283&e?12241&e?en/dover.aspx	Block	1
79.183.107.232	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/xmlrpc.php	Block	1
213.57.44.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
195.154.168.82	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
2.54.147.250	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.86.75.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
208.90.57.196	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
46.117.181.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.55.241	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 213.57.55.241 (Open Mode)	None	1
72.79.45.182	United States	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1515-he/atal.aspx	Block	1
195.154.226.90	France	147.237.77.74	law.idf.il	Illegal HTTP Version HTTP/	Block	1
37.60.44.61	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.60.44.61	Block	1
141.101.17.201	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/iturim/resources/images/body/images/main.jpg	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
66.249.66.127	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/900-he/x?x'xE x"x~x>x x• x&x•x'x™x" x•x"x&x•x'x™x x~x™x§x".aspx	Block	1
176.13.4.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
47.88.13.149	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/forums/ajax/api/hook/decodearguments	Block	1
83.99.192.91	Latvia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/band	Block	1
213.57.55.241	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.125.4.74	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method	Block	1