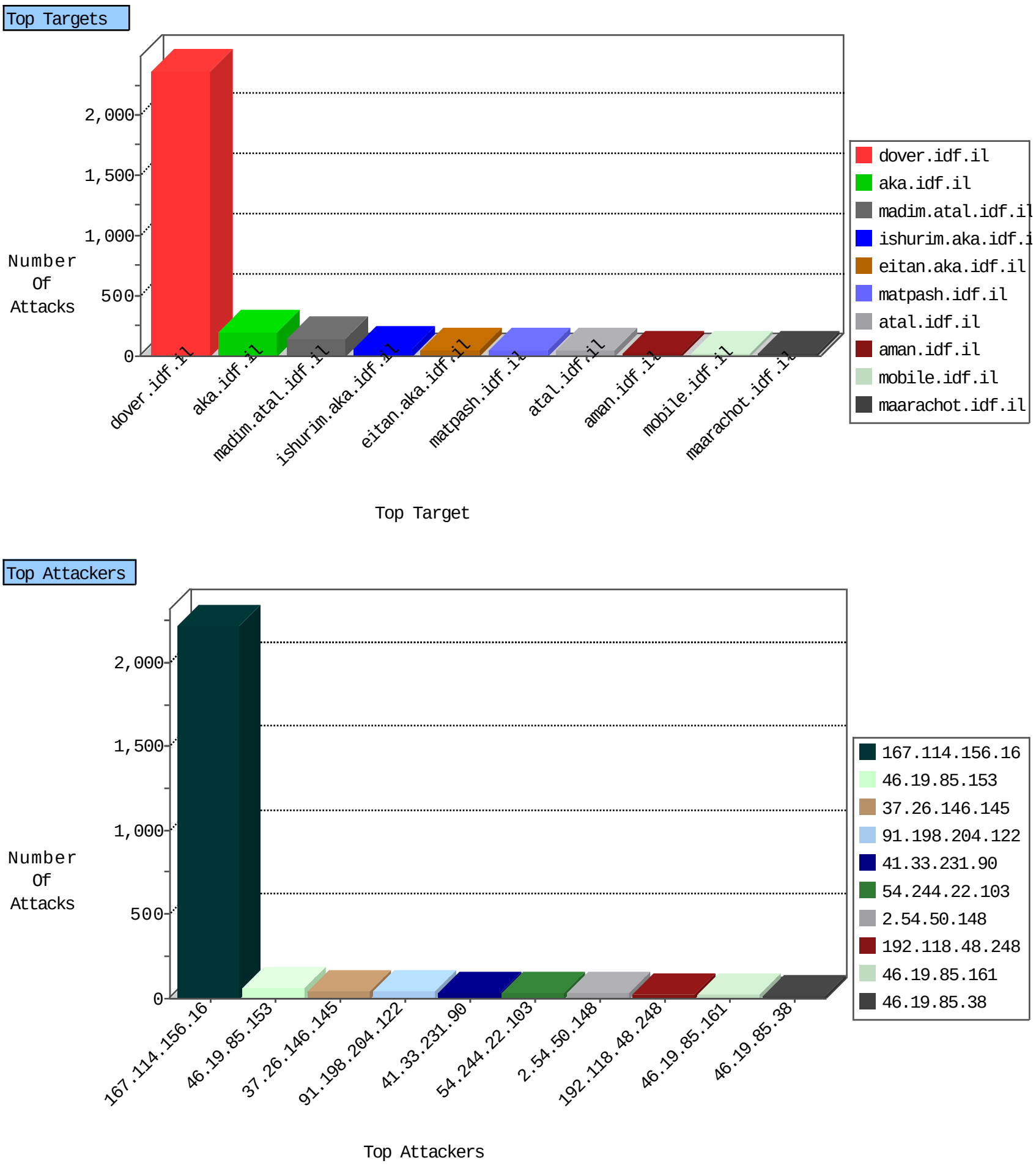
01-21-2016-08:04:05 to 01-21-2016-09:04:05

IDF Under Attack Daily Report



01-21-2016-08:04:05 to 01-21-2016-09:04:05

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	3014
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	212
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
159.104.163.19	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
146.185.239.100	Russian Federation	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
159.104.163.20	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.104.163.17	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
74.91.28.61	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
159.104.163.18	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
142.54.169.166	United States	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1

01-21-2016-08:04:05 to 01-21-2016-09:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
185.32.179.208	Israel	147.237.72.167	ishurim.aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-21-2016-08:04:05 to 01-21-2016-09:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.14.201	147.237.72.167	Israel	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
167.61.79.124	147.237.0.35	Uruguay	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
118.70.81.24	147.237.77.233	Vietnam	atal.idf.il	ET SCAN Potential SSH Scan	1
118.70.81.24	147.237.77.178	Vietnam	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
118.70.81.24	147.237.77.19	Vietnam	law-forum.idf.il	ET SCAN Potential SSH Scan	1
118.70.81.24	147.237.76.147	Vietnam	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.57	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.159.139.63	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.21.57	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.85.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
118.70.81.24	147.237.77.234	Vietnam	halag.idf.il	ET SCAN Potential SSH Scan	1
118.70.81.24	147.237.77.212	Vietnam	e.dover.idf.il	ET SCAN Potential SSH Scan	1
118.70.81.24	147.237.77.170	Vietnam	maarachot.idf.il	ET SCAN Potential SSH Scan	1
118.70.81.24	147.237.76.200	Vietnam	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
118.70.81.24	147.237.0.19	Vietnam	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.57	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.181.102.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.237	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1

01-21-2016-08:04:05 to 01-21-2016-09:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.146.145	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
91.198.204.122	Denmark	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	46
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	36
46.19.85.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
192.118.48.248	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.3	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.118.48.248	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.169	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	9
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.100.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.199.251.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.86.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.131.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
188.161.247.65	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.22.131.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.150.189.2	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	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
2.54.149.87	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.21.45	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.57.215.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
217.194.203.238	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.106.46.74	Palestinian Territory Occupied	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
80.179.114.27	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
80.179.114.27	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.81.241.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.194.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
62.219.168.110	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
84.111.196.22	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
213.8.204.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.54.16.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.40.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.215.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.204.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.253.144.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.114.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.147.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.66.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.24.102	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
109.253.145.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.171	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
141.8.184.5	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
2.54.50.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
80.246.139.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
185.32.179.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
2.54.32.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.66.18.230	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.66.18.230	Block	6
185.13.193.36	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	4
176.13.11.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.13.193.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.145.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.8.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.24.102	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 79.177.24.102	Block	2
2.54.4.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.123.29.92	Moldova, Republic of	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
149.88.106.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
82.80.133.53	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
46.19.85.154	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.180.114.186	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
176.123.29.92	Moldova, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/blog/xmlrpc.php	Block	1
157.55.39.160	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
74.91.28.61	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to www.366901.com/	Block	1
62.219.13.180	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
104.128.144.131	Canada	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
5.29.47.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.110.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
2.52.132.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
109.66.18.230	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
82.80.133.53	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
46.19.85.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.5	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15003-he/mmmmmmm=d507d3e0mmmmmmm_d507d3e0	Block	1
80.82.65.82	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
176.10.104.243	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
77.42.252.199	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
66.249.64.70	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter lang in www.eitan.aka.idf.il/938-en/eitan.aspx	None	1
104.128.144.131	Canada	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
37.26.148.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.117.14.194	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
81.218.251.252	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.178.110.143	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
2.54.2.12	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
176.13.15.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.100.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.79.218	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
85.10.210.199	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.86.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1