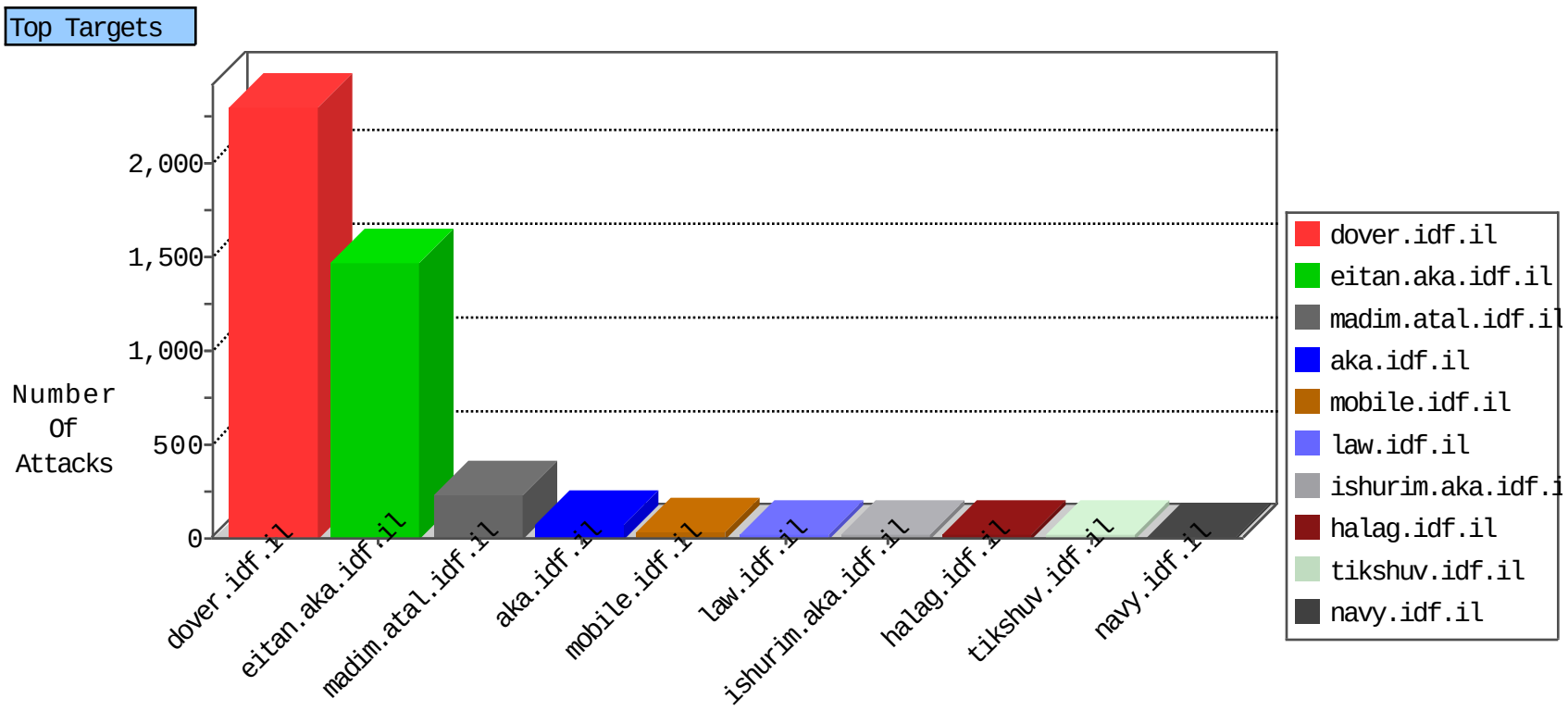
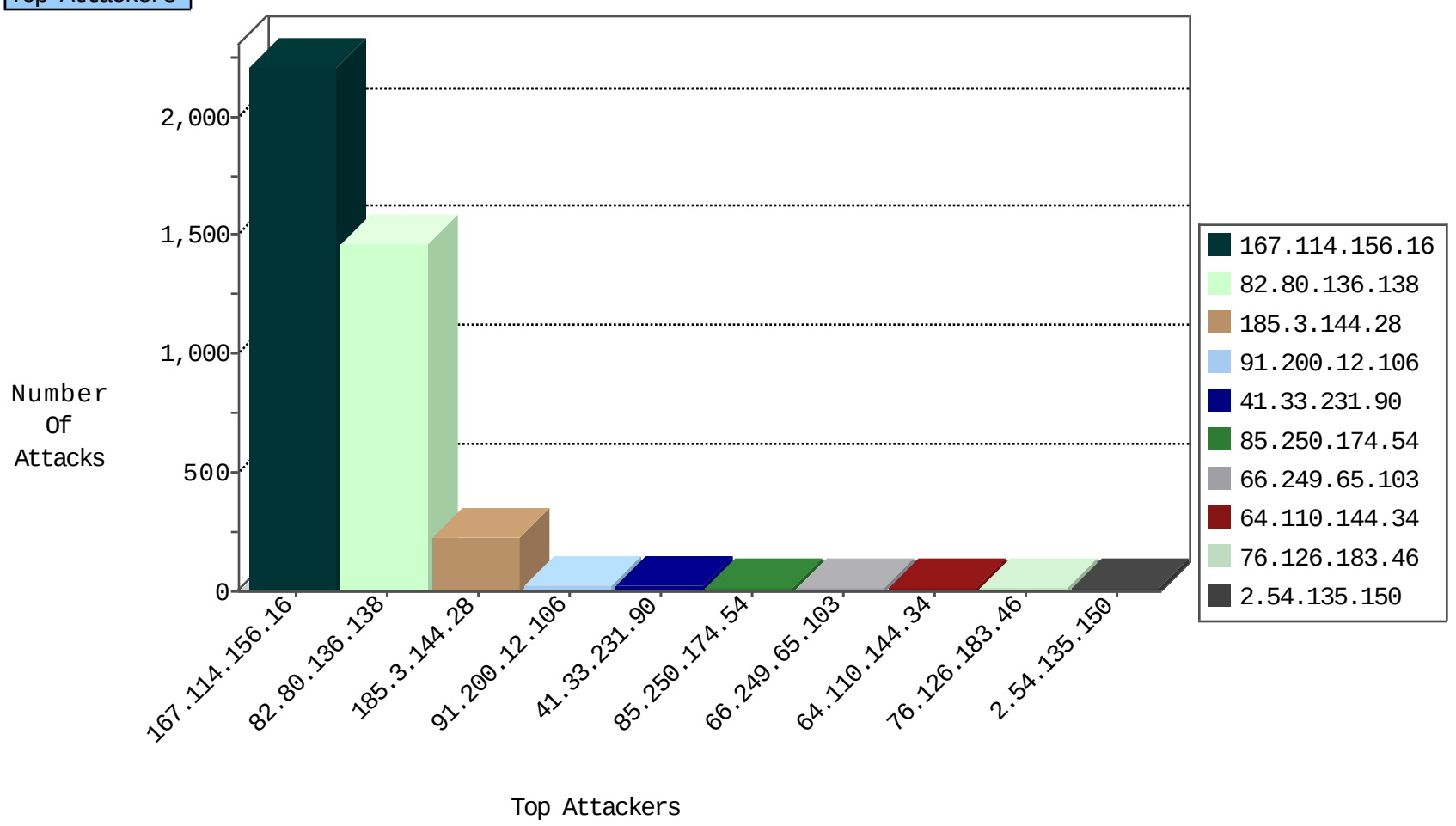
12-13-2015-01:04:09 to 12-13-2015-02:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



12-13-2015-01:04:09 to 12-13-2015-02:04:09

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	3545
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
109.188.126.44	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
115.239.228.8	China	147.237.0.35	akaws.idf.il	Frk_Under_Attack_Con_Http	drop	2
113.70.177.101	China	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	2
115.239.228.8	China	147.237.0.35	akaws.idf.il	Frk_Purple_Con_Limit_Http	drop	1
49.71.227.201	China	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
116.17.23.163	China	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
113.85.163.130	China	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
123.164.89.246	China	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
66.240.236.119	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

12-13-2015-01:04:09 to 12-13-2015-02:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.75.220.155	Netherlands	147.237.77.243	mobile.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
27.5.180.194	India	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
94.75.220.155	Netherlands	147.237.77.179	e.mazi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
94.75.220.155	Netherlands	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

12-13-2015-01:04:09 to 12-13-2015-02:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
93.158.215.56	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.181	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
121.235.208.152	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
117.31.224.80	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
115.182.17.13	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
109.235.254.181	147.237.76.86	Turkey	navy.idf.il	ET SCAN NMAP -sS window 1024	1
94.75.220.155	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
94.75.220.155	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.215.56	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
177.245.59.93	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
42.96.203.166	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
118.112.185.236	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
115.182.17.13	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
109.235.254.181	147.237.76.86	Turkey	navy.idf.il	ET SCAN NMAP -sS window 4096	1
98.119.105.221	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
94.75.220.155	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.215.56	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1

12-13-2015-01:04:09 to 12-13-2015-02:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.80.136.138	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1314
66.249.65.103	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
2.54.135.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
76.126.183.46	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
64.110.144.34	Italy	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.29.75.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
207.46.13.48	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	7
149.88.4.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.241.226.39	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	6
207.46.13.1	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.250.174.54	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.250.174.54	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
65.55.210.104	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.67.98.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.24.247	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
82.80.62.155	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.176.119.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
92.96.74.124	United Arab Emirates	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
79.180.18.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.237.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.148.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
92.96.74.124	United Arab Emirates	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
80.178.215.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.26.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.5.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.154.227.118	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
40.77.167.89	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2
85.250.174.54	Israel	147.237.0.34	tikshuv.idf.il	Spoofed Reset		monitor	2
207.241.226.39	United States	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	2
84.108.67.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.65.106	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.250.174.54	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid sequence number	alert	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
207.46.13.142	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
177.235.243.83	Brazil	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
68.180.228.112	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
85.250.176.40	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
218.22.211.69	China	147.237.76.34	yohalan.idf.il	drop		drop	1
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.108.67.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.199	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
94.44.252.79	Hungary	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
185.3.144.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
71.224.80.88	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.136.138	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	146
185.3.144.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
185.3.144.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	64
185.3.144.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	32
91.200.12.106	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	12
91.200.12.106	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 91.200.12.106	Block	11
2.54.148.18	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.148.18	Block	7
109.65.3.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
199.30.24.33	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
76.78.240.148	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	2
93.173.28.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	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	1
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	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
72.49.7.83	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
54.152.228.19	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/rights/asp/info.asp	None	1
94.185.83.100	Sweden	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on testp4.pospr.waw.pl/testproxy.php	Block	1
85.65.231.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
66.249.66.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
91.200.12.106	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/592-4071-en/index.php	Block	1
72.49.7.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.65.18	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
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	1
91.196.50.33	Poland	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
66.249.66.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	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
2.54.148.18	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	1
174.49.73.68	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/idf_in_pictures/2002/april/1.stm	Block	1
91.200.12.137	Ukraine	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
199.30.25.191	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8920-he/refuah.aspx	Block	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
91.196.50.33	Poland	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
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	1
37.142.97.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.179.210.163	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	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
66.249.66.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/atuda	Block	1
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	1
66.249.66.181	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
94.185.83.100	Sweden	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on testp4.pospr.waw.pl/testproxy.php	Block	1

12-13-2015-01:04:09 to 12-13-2015-02:04:09