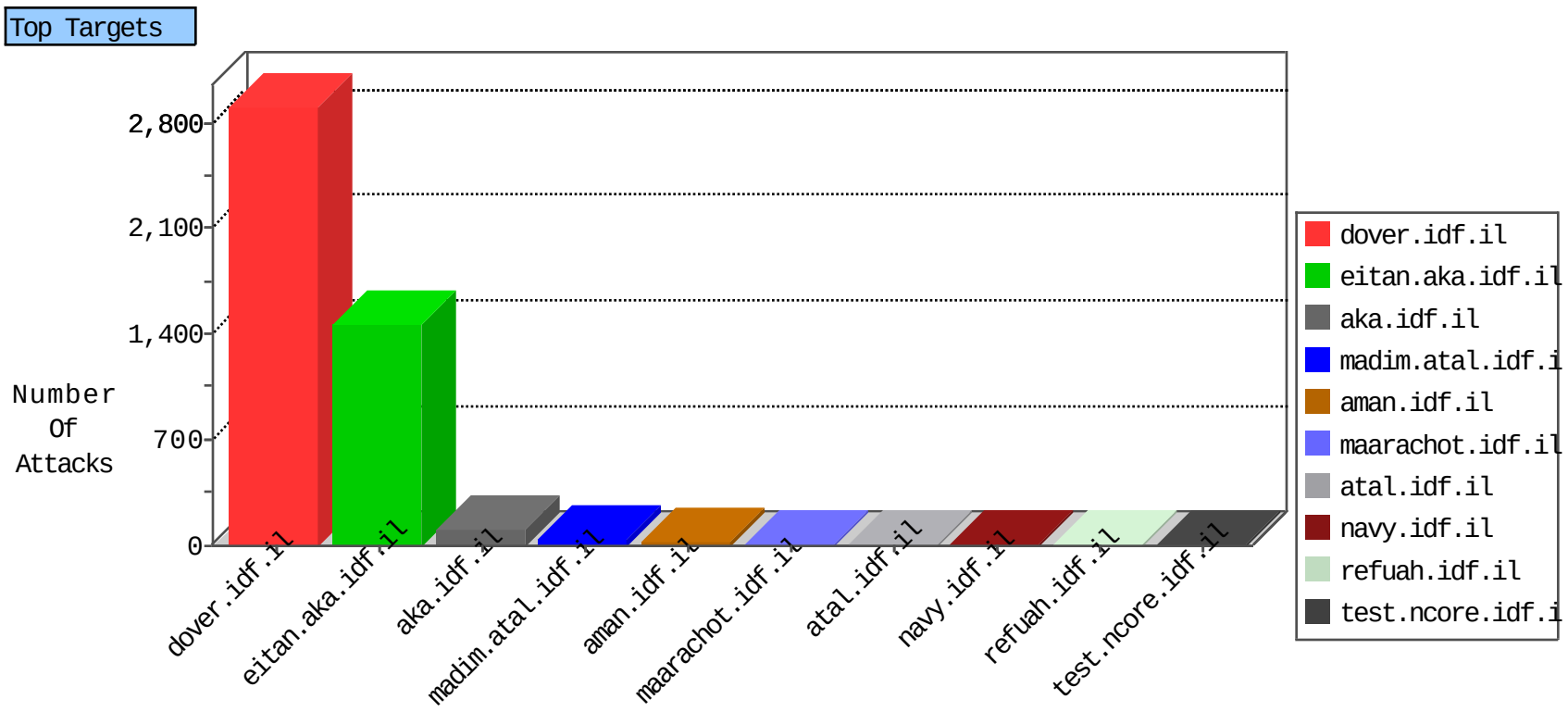
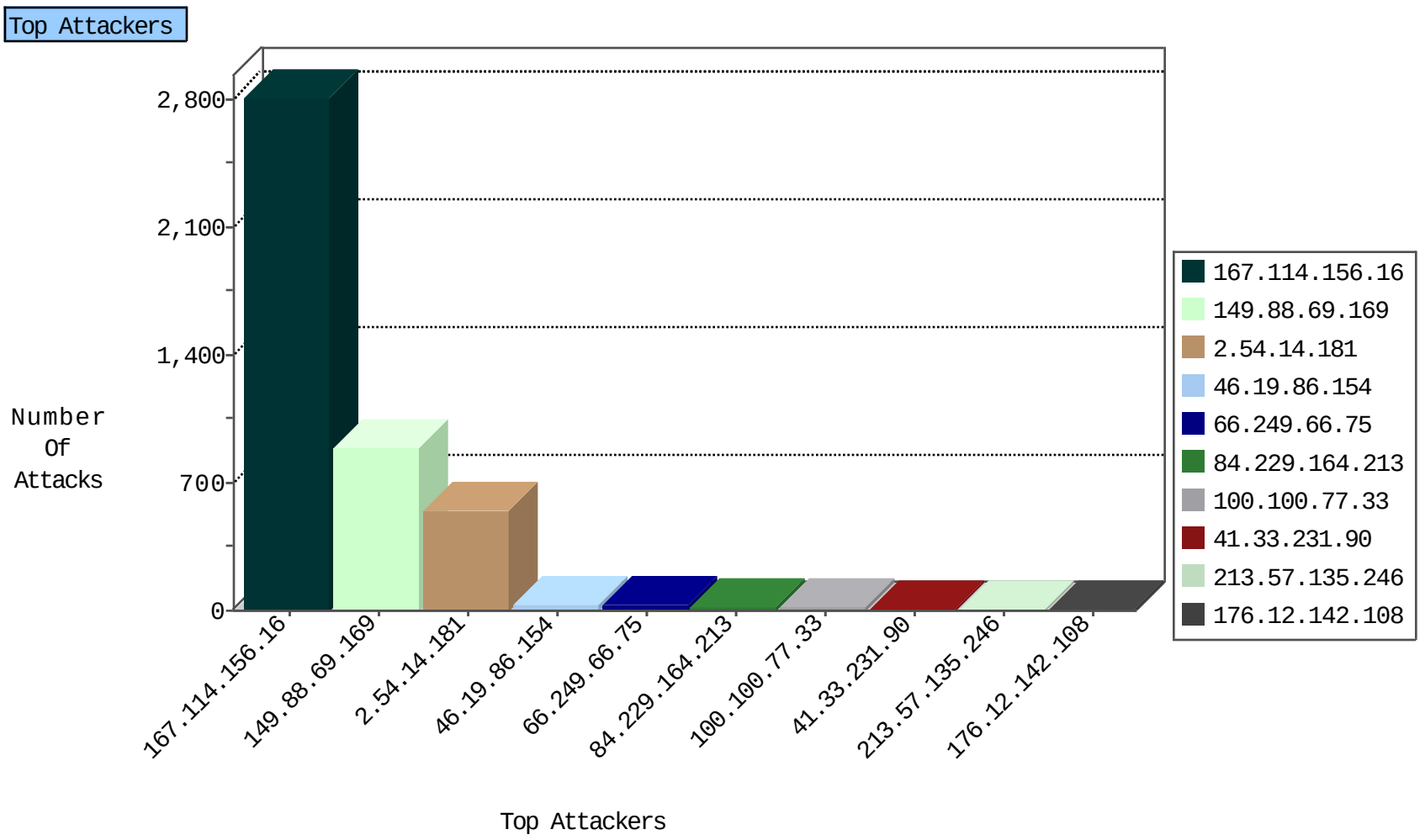
12-01-2015-06:04:01 to 12-01-2015-07:04:01

IDF Under Attack
Daily Report

Top Targets



Top Attackers



12-01-2015-06:04:01 to 12-01-2015-07:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	8191
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3654
115.239.228.8	China	147.237.76.176	test.ncore.idf.il	JLM_Purple_Con_Limit_Http	drop	3
79.182.217.248	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.8	China	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Http	drop	2
213.57.128.79	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
202.112.51.96	China	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1
81.4.217.170	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.71	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
93.158.203.169	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

12-01-2015-06:04:01 to 12-01-2015-07:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-01-2015-06:04:01 to 12-01-2015-07:04:01

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	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
171.232.56.152	147.237.0.16	Vietnam	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	4
66.249.66.78	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
222.21.43.56	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
109.235.254.181	147.237.77.121	Turkey	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
222.21.43.56	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
82.192.90.145	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
204.151.29.209	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
196.47.173.21	147.237.76.44	Cote D'Ivoire	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
31.6.71.154	147.237.77.121	Poland	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
23.92.216.183	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 2048	1
151.11.201.3	147.237.77.233	Italy	atal.idf.il	ET SCAN NMAP -sS window 3072	1
222.21.43.56	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.21.43.56	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.21.43.56	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
82.192.90.145	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
210.50.197.154	147.237.77.233	Australia	atal.idf.il	ET SCAN NMAP -sS window 3072	1
82.192.90.145	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
204.151.29.209	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.76.44	Cote D'Ivoire	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
31.6.71.154	147.237.72.14	Poland	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
180.97.106.162	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
23.92.216.183	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -f -sS	1
151.11.201.3	147.237.77.233	Italy	atal.idf.il	ET SCAN NMAP -sS window 4096	1
119.193.20.208	147.237.77.19	Korea, Republic of	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.21.43.56	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

12-01-2015-06:04:01 to 12-01-2015-07:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.14.181	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	549
149.88.69.169	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
84.229.164.213	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	23
172.56.5.196	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	5
213.57.135.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
213.57.135.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
65.55.210.37	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.24.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.173.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.144	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.54.140.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
100.100.72.73		147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	3
79.177.128.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
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
46.19.85.198	Israel	147.237.72.166	aka.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
84.109.131.81	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.120.255.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.75.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
62.210.209.237	France	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
207.46.13.4	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
213.172.183.61	Poland	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
77.237.138.51	Czech Republic	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.22.131.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
216.218.206.108	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
8.37.228.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
84.108.29.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
213.57.128.79	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
1.144.96.113	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.59	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.120.255.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
123.125.71.111	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
84.110.35.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.91	United States	147.237.0.33	idf.il	drop		drop	1
5.22.134.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
203.143.23.137	Sri Lanka	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.142	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
24.161.47.154	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.60	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.224	United States	147.237.77.227	e.hamaz.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
149.88.69.169	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 149.88.69.169	Block	860
46.19.86.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
176.12.142.108	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	7
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	2
66.249.66.28	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.28	Block	2
176.12.137.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.160.241.31	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
40.77.167.34	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/sip_storage/files/4/68624	Block	1
208.115.113.89	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
79.179.110.41	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	1
192.116.54.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-16893-he/dover.aspx	Block	1
59.88.217.39	India	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
157.55.39.55	United States	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
84.109.131.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.148.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19798-he/idfgdover.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
141.212.122.128	United States	147.237.76.42	refuah.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
40.77.167.38	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/z516518/svc/getsuggestcontent/6867784	Block	1
208.115.113.89	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 208.115.113.89	Block	1
79.182.147.112	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
59.88.217.39	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
157.55.39.55	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/auth_img.php	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
37.142.64.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international-training	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
176.12.149.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.31	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1086-en/dover.aspx	Block	1
46.19.85.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.148.114	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	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
80.246.136.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 195.154.227.118	Block	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/3238.jpg	Block	1
157.55.39.76	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/moreinfo/tichnun.yosh@gmail.com	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
37.142.68.59	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
207.46.13.173	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.173	Block	1
79.177.48.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.15.186	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	Distributed Unauthorized URL Access on 147.237.77.216/1133-16893-he/dover.aspx	Block	1
149.88.69.169	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	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
81.218.208.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/haredim/general.aspx	None	1