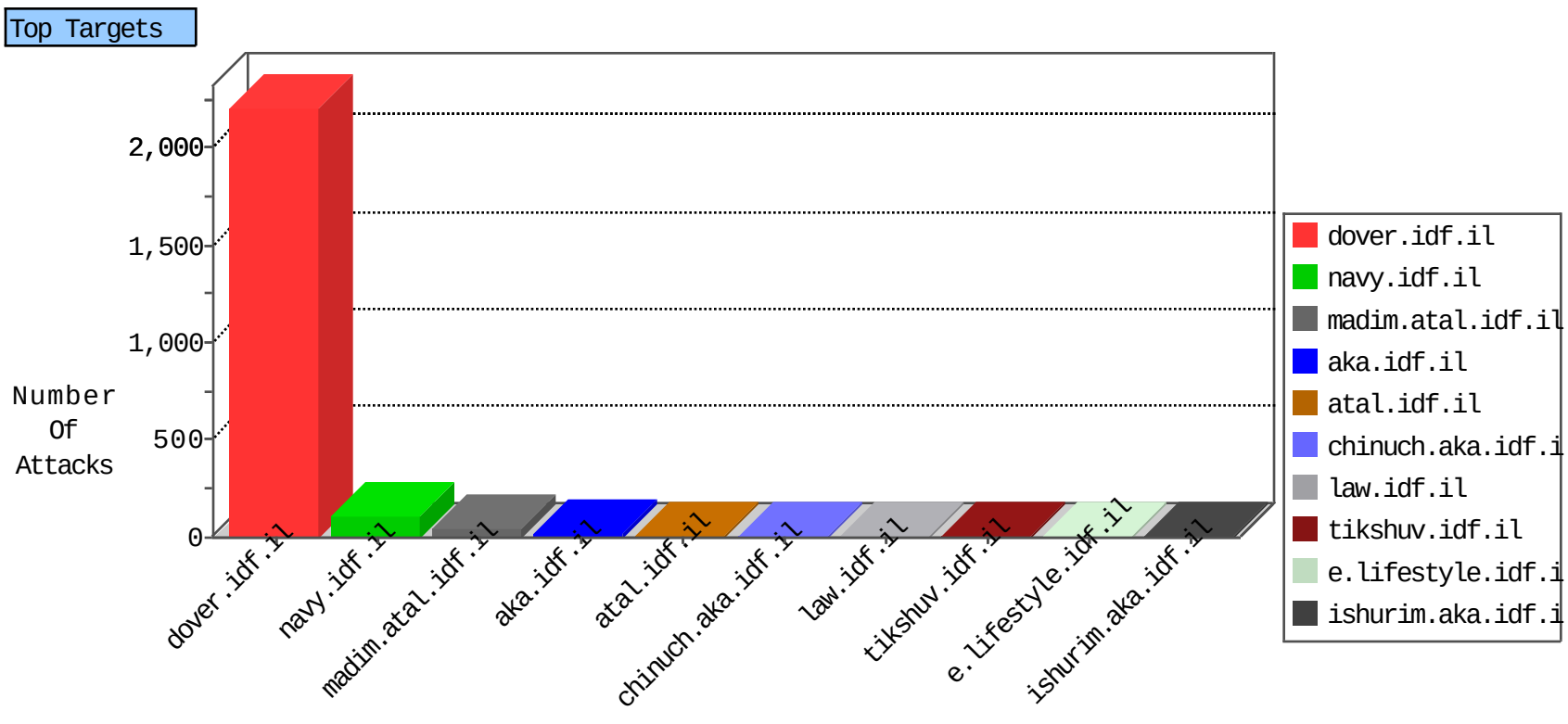
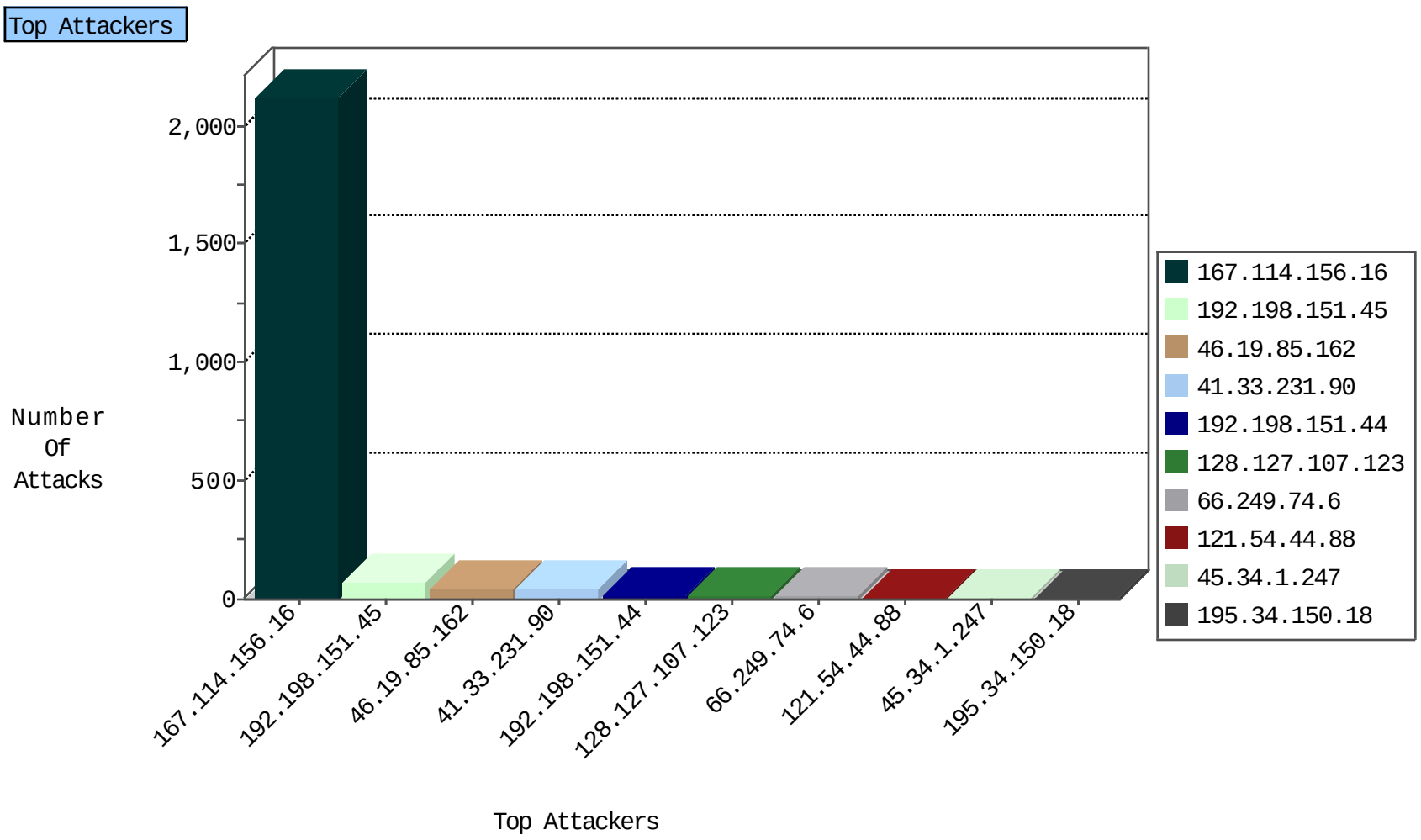
12-28-2015-04:04:01 to 12-28-2015-05:04:01

IDF Under Attack
Daily Report

Top Targets



Top Attackers



12-28-2015-04:04:01 to 12-28-2015-05:04:01

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	3173
192.198.151.45	Europe	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
192.198.151.45	Europe	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
192.99.131.107	Canada	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
39.183.43.237	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
192.99.131.107	Canada	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
39.183.43.237	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
192.99.131.107	Canada	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

12-28-2015-04:04:01 to 12-28-2015-05:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-28-2015-04:04:01 to 12-28-2015-05:04:01

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
151.217.176.25	147.237.76.202		e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.88	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
146.185.250.2	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.88	147.237.8.28		e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
73.17.14.46	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.63	147.237.77.227		e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.34.1.247	147.237.76.198		e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.63	147.237.76.177		ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.34.1.247	147.237.76.147		chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.63	147.237.76.42		refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.34.1.247	147.237.76.39		mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.55	147.237.76.86		navy.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
45.34.1.247	147.237.0.200		m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.55	147.237.72.14		dover.idf.il(old)	ET SCAN Potential VNC Scan 5800-5820	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
151.217.176.25	147.237.77.235		sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.88	147.237.77.121		e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.176.25	147.237.8.27		e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.88	147.237.8.46		e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
120.71.134.156	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
151.217.178.68	147.237.72.167		ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.151.52.16	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.63	147.237.76.202		e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.34.1.247	147.237.76.196		e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.63	147.237.76.148		gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.34.1.247	147.237.76.44		e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.63	147.237.8.50		e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.34.1.247	147.237.76.31		nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.55	147.237.72.167		ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
211.155.16.154	147.237.8.24	China	e.lifestyle.idf.il	GPL SCAN nmap TCP	1
45.34.1.247	147.237.0.34		tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.36	147.237.76.148		gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.77.216		dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

12-28-2015-04:04:01 to 12-28-2015-05:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
192.198.151.45	Europe	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	63
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
192.198.151.44	Europe	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	15
66.249.74.6	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
121.54.44.88	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
213.57.135.165	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.247.36.78	Netherlands	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
128.127.107.123	Netherlands	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
128.127.107.123	Netherlands	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
128.127.107.123	Netherlands	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
128.127.107.123	Netherlands	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
172.56.4.61	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
128.232.110.28	United Kingdom	147.237.0.35	akaws.idf.il	drop		drop	2
108.184.44.161	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
166.172.62.52	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
52.33.66.29	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
66.249.74.12	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
65.55.212.74	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
128.127.107.123	Netherlands	147.237.0.15	kosher-kravi.idf.i	drop	First packet isn't SYN	drop	1
184.105.247.203	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
67.227.163.231	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.161	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
81.18.165.229	Netherlands	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.100	United States	147.237.0.35	akaws.idf.il	drop		drop	1
65.55.212.85	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
149.88.86.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.54.5.173	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.107	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.124	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.127.107.123	Netherlands	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.251	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
70.194.143.44	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.75	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
141.212.122.162	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.115.113.84	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
184.105.139.112	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
65.55.218.34	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.108	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
190.54.212.193	Chile	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.34	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.92	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.168	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
131.253.26.232	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
121.54.44.88	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.112	United States	147.237.77.176	matpash.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
46.19.85.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.19.85.162	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
46.19.86.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
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
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	2
207.46.13.134	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
201.148.104.107	Chile	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19716-he/kkkkkkk=16e4bc31kkkkkkk_16e4bc31	Block	1
91.228.248.251	Israel	147.237.0.34	tikshuv.idf.il	Suspicious Response Code	Block	1
197.221.14.17	South Africa	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
128.127.107.123	Netherlands	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
201.148.104.107	Chile	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
180.76.15.13	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
216.218.206.66	United States	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/size100x0/3469.jpg	Block	1
197.221.14.17	South Africa	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
141.8.142.82	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	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
180.76.15.155	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
200.97.215.3	Brazil	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
141.212.122.97	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /x	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.120.142.235	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
207.46.13.109	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter date in www.eitan.aka.idf.il/cdn/allmenus/css/all_monochrome.css	None	1
186.202.127.23	Brazil	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/size100x0/3241.jpg	Block	1
200.97.215.3	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
40.77.167.8	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 40.77.167.8	Block	1
176.13.8.89	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
84.108.60.72	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
46.166.137.195	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
186.202.127.23	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
109.201.154.181	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1