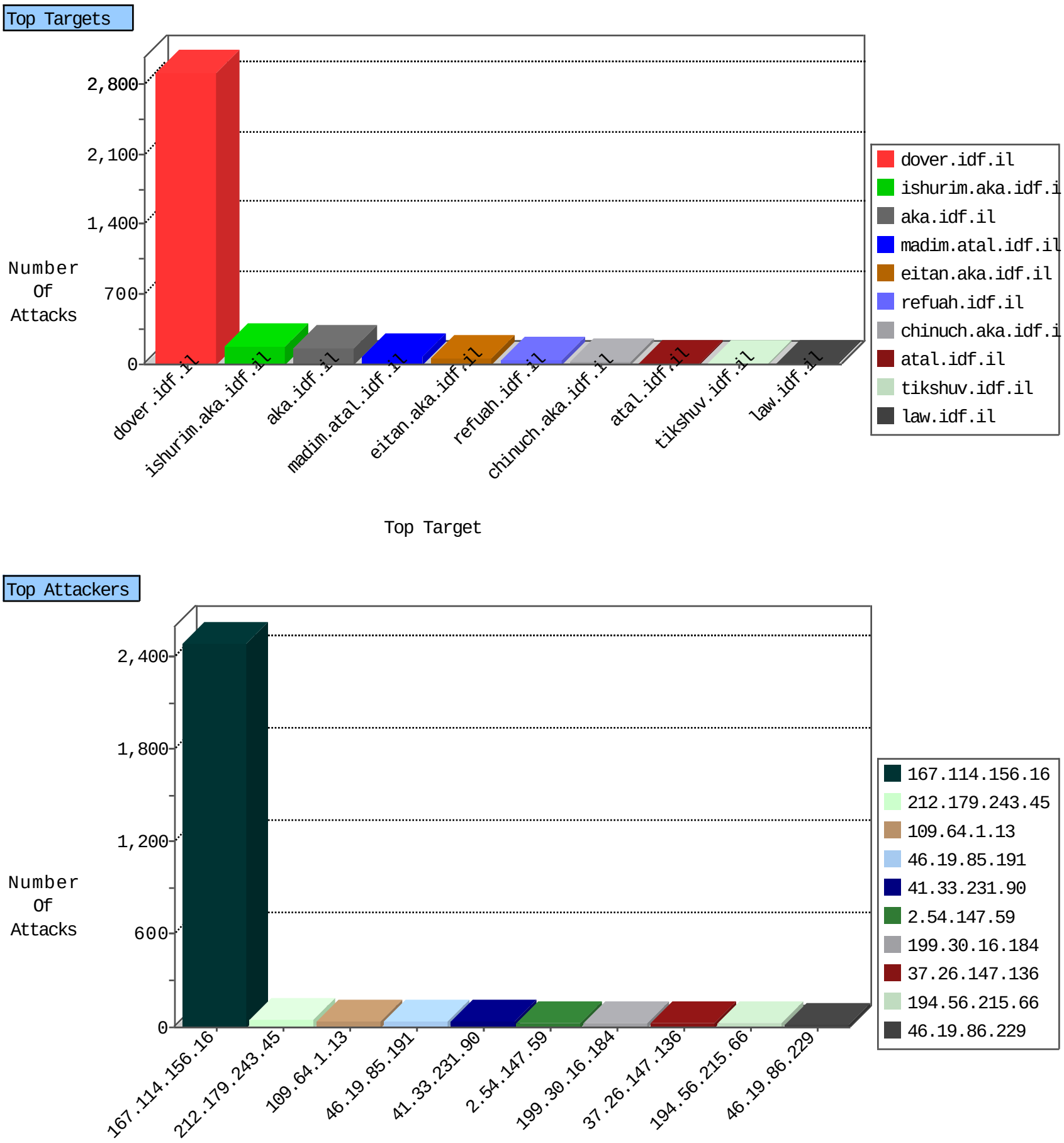
12-22-2015-10:04:02 to 12-22-2015-11:04:02

IDF Under Attack
Daily Report



12-22-2015-10:04:02 to 12-22-2015-11:04:02

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	3342
63.141.217.231	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
183.60.48.25	China	147.237.76.198	e.yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
204.42.253.130	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	2
222.44.214.66	China	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
222.44.214.66	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
222.220.43.216	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
87.97.125.74	Hungary	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
222.220.43.216	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
88.253.26.242	Turkey	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

12-22-2015-10:04:02 to 12-22-2015-11:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.191	France	147.237.77.226	www.chamatz.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

12-22-2015-10:04:02 to 12-22-2015-11:04:02

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	3
169.54.244.84	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.130.188.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
169.54.244.84	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
71.6.135.131	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
169.54.244.84	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
62.128.45.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
169.54.244.78	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
46.19.85.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
169.54.244.78	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential VNC Scan 5800-5820	1
37.26.147.241	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.53.239	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
166.63.122.229	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
182.75.6.126	147.237.76.177	India	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
109.186.120.213	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
169.54.244.84	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
92.222.242.108	147.237.77.227	France	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.244.84	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
71.6.135.131	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
169.54.244.84	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.78.69	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
169.54.244.78	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
46.19.86.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
169.54.244.78	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
37.142.229.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
169.54.244.78	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
2.54.20.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
166.63.122.229	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
134.213.133.4	147.237.77.74	United Kingdom	law.idf.il	ET SCAN NMAP -sS window 3072	1
181.103.240.157	147.237.77.216	Argentina	dover.idf.il	portscan: TCP Distributed Portscan	1
92.222.242.108	147.237.77.234	France	halag.idf.il	ET SCAN NMAP -sS window 1024	1

12-22-2015-10:04:02 to 12-22-2015-11:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.243.45	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
109.64.1.13	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.85.191	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	31
46.19.86.229	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
194.56.215.66	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	12
194.56.215.66	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.127	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
37.26.148.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
46.19.85.174	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.145	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
46.121.45.2	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.54.147.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.147.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.147.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.147.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
46.19.85.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.118	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
89.138.176.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
188.120.148.232	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.180	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
176.12.146.4	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.117.3.254	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.196.42.196	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
63.141.217.231	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.253.135.201	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
180.183.6.209	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
217.194.194.104	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.72	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
176.12.146.4	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.229	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
193.43.246.250	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4

12-22-2015-10:04:02 to 12-22-2015-11:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.30.16.184	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	25
37.26.147.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
46.19.86.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
46.19.86.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	8
37.26.149.153	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	7
176.13.19.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
37.142.68.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.19.86.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
207.46.13.1	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.66.147.153	Israel	147.237.77.176	matpash.idf.il	Parameter Type Violation search in www.cogat.idf.il/1035-he/cogat.aspx	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
217.164.217.96	United Arab Emirates	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
176.12.151.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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	2
37.26.147.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.132.13	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
196.22.142.216	South Africa	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.i	Unknown Parameter l in www.chinuch.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
2.54.142.107	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.229.131.191	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
50.87.248.143	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
173.252.73.112	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.137.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	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
79.180.203.149	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl37 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
198.154.225.251	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
46.19.85.45	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
122.3.142.91	Philippines	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
70.39.151.172	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
185.32.179.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
10.162.90.64		147.237.76.30	himush.idf.il	Unknown Parameter amp;rnd in www.chimush.atal.idf.il/shared/ajax/createcaptchaimage.aspx	None	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
2.52.40.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.190.100.236	Iceland	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
50.62.176.14	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
176.13.11.57	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
151.80.101.138	Italy	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/8/3688.pdf</p>	Block	1
79.183.101.136	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
79.177.222.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
196.22.142.216	South Africa	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/)	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/kkkkkkk=1daa96abkkkkkkk_1daa96ab	Block	1
2.54.158.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.203.79	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
46.120.98.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-22-2015-10:04:02 to 12-22-2015-11:04:02