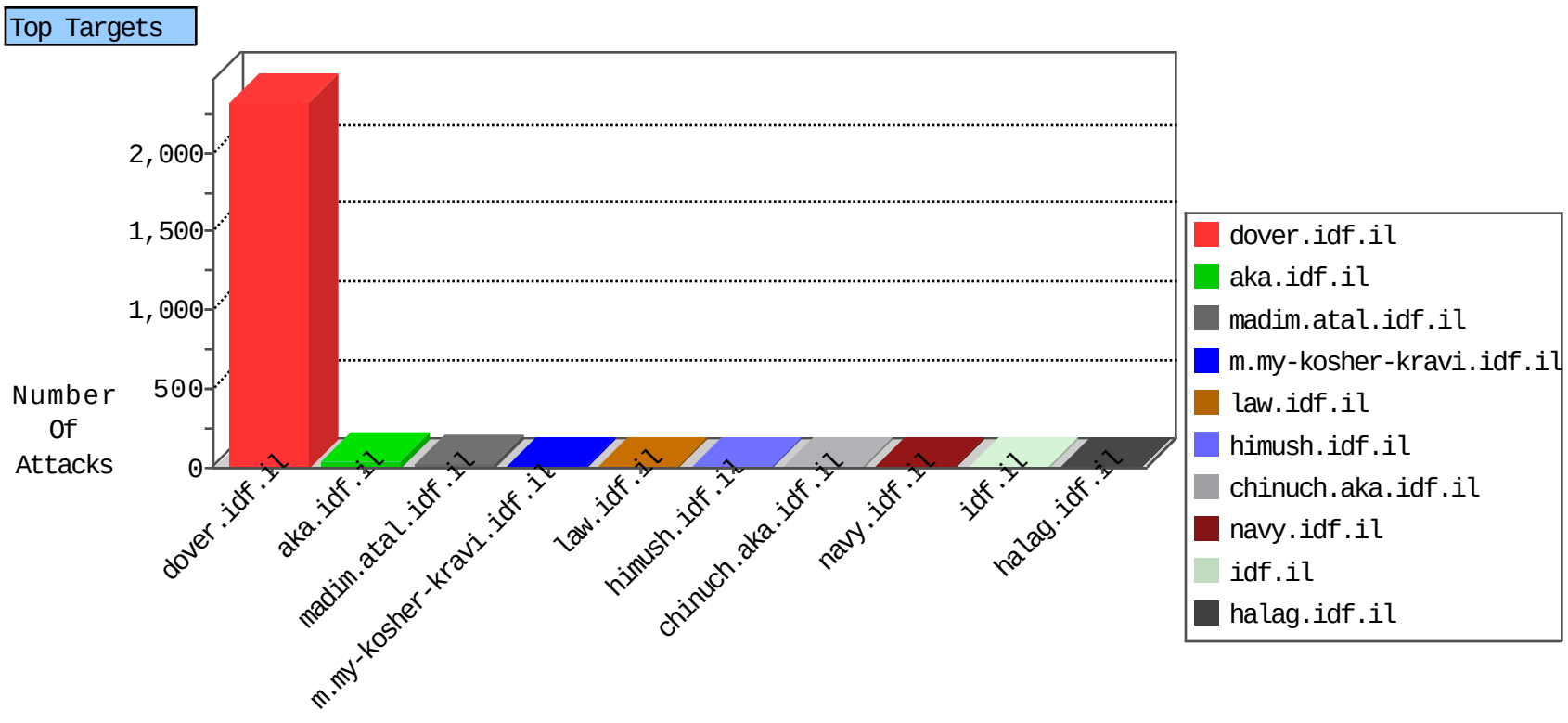
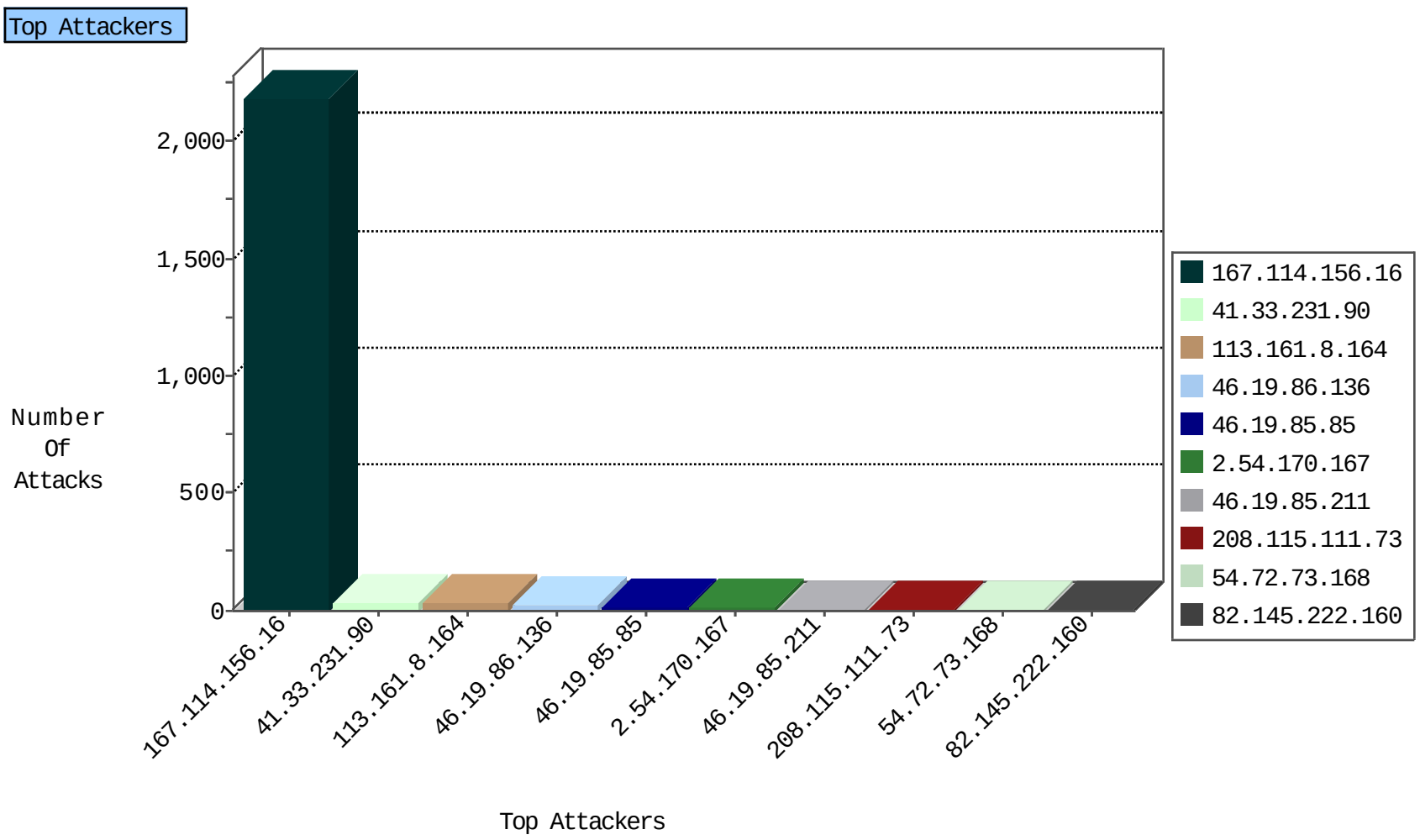
12-08-2015-06:04:03 to 12-08-2015-07:04:03

IDF Under Attack
Daily Report





12-08-2015-06:04:03 to 12-08-2015-07:04:03

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	3357
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	486
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
185.35.62.37	Switzerland	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

12-08-2015-06:04:03 to 12-08-2015-07:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-08-2015-06:04:03 to 12-08-2015-07:04:03

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
66.249.80.105	147.237.76.86	Australia	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.22	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.82	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
180.97.106.161	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.39	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
159.122.238.133	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
151.11.201.3	147.237.76.200	Italy	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
107.150.19.184	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
107.150.19.184	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
209.126.116.147	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.76.196	Turkey	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.162	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
5.135.139.53	147.237.77.74	France	law.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	1
159.122.238.133	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
151.11.201.3	147.237.76.200	Italy	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
107.150.19.184	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
221.160.105.136	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
98.119.105.221	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
198.20.69.98	147.237.76.30	United States	himush.idf.il	ET DROP Dshield Block Listed Source	1
82.117.208.243	147.237.8.45		e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
187.246.11.226	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

12-08-2015-06:04:03 to 12-08-2015-07:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
113.161.8.164	Vietnam	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
2.54.170.167	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
113.161.8.164	Vietnam	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.145.222.160	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
66.249.93.202	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.148.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.67.144.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.16.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
82.80.16.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
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
208.115.111.73	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	2
95.35.74.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.85.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
216.218.206.83	United States	147.237.0.33	idf.il	drop		drop	1
62.0.34.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.80	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.78.143.241	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.24	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
179.225.145.185	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.131	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.116	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
62.0.34.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.35	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.70	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.139.67	United States	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
141.212.122.135	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.88.54.116	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
115.230.124.164	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
74.82.47.35	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.75	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.75	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.54.170.167	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.136	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.73	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
141.212.122.128	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.47	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.75	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

12-08-2015-06:04:03 to 12-08-2015-07:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.136	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	25
176.13.15.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.2.198	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtPersonalId in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	3
176.12.147.199	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
176.13.18.71	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
176.12.151.28	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
185.32.179.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
138.134.102.15	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 138.134.102.15	Block	1
67.80.11.1	United States	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/mobile/	Block	1
188.138.17.205	France	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/robots.txt	Block	1
157.55.39.112	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	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
195.62.53.168	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to /css/css	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-he/dover.aspx	Block	1
8.37.70.37	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1134-he/atal.aspx&usg=alkjrhhbshhaq4xygksbm-epy2capidxg	Block	1
138.134.102.15	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/4/size338x0/1564.jpg	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
213.57.215.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/brothers/news/default.asp	Block	1
188.143.232.34	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 188.143.232.34	Block	1
109.66.141.201	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.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
66.249.66.39	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
8.37.71.13	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/1097-he/halag.aspx&usg=alkjrhgpuyd7ywn2uh7mewhnmsw6tayjqg	Block	1
141.212.122.129	United States	147.237.76.30	himush.idf.il	Malformed URL proxytest.zmap.io:80	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
188.143.232.34	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/searchresults/searchresults.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.66.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	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
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
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
37.26.146.187	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
141.212.122.129	United States	147.237.76.147	chinuch.aka.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
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	1
188.143.232.37	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation PageNumber in www.tikshuv.idf.il/modules/forums/searchresults.aspx	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 66.249.66.25	Block	1
176.13.2.198	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding G/iO(Hzu%$alq>&Suu1ZQX in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
113.161.8.164	Vietnam	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	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
66.249.66.78	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
157.55.39.112	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	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
188.143.232.37	Russian Federation	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1

12-08-2015-06:04:03 to 12-08-2015-07:04:03