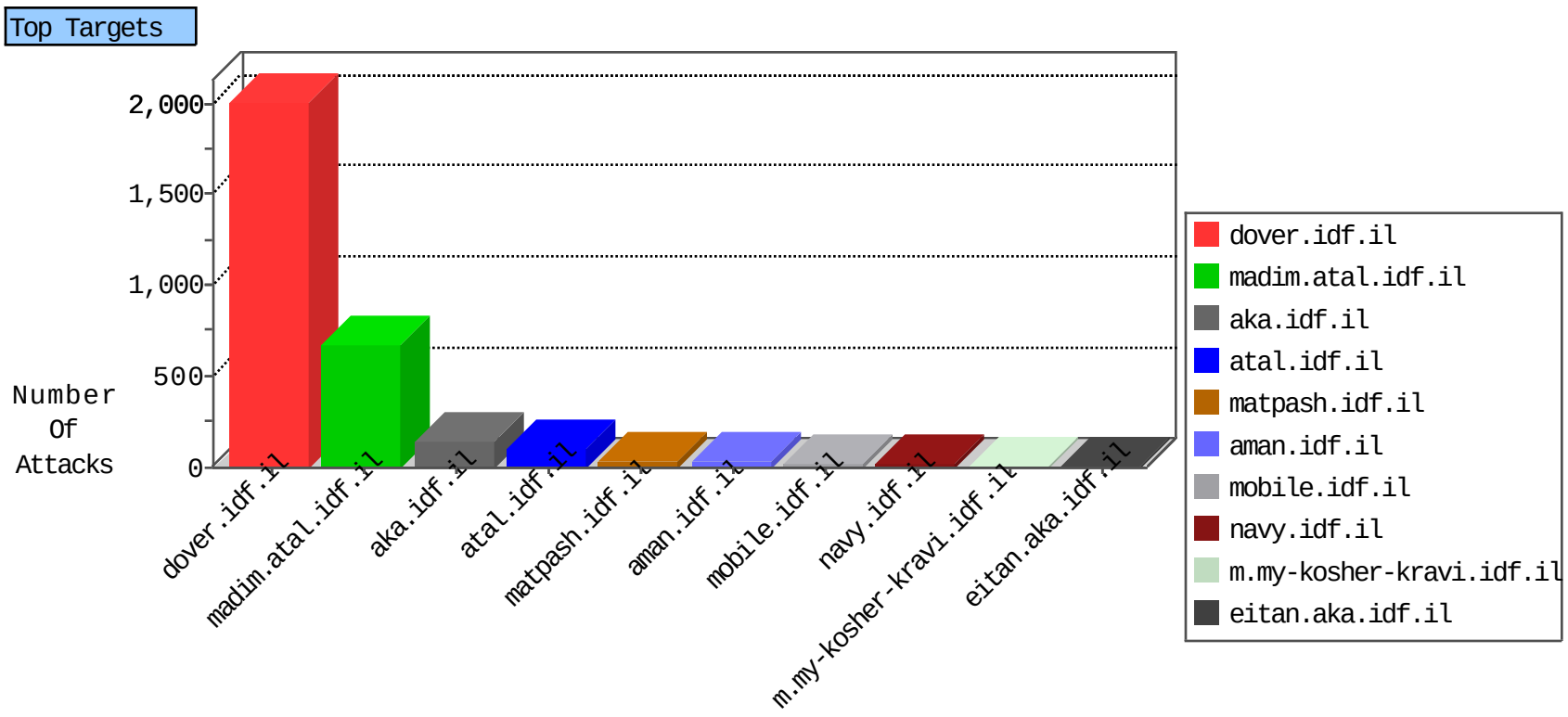
12-26-2015-14:04:04 to 12-26-2015-15:04:04

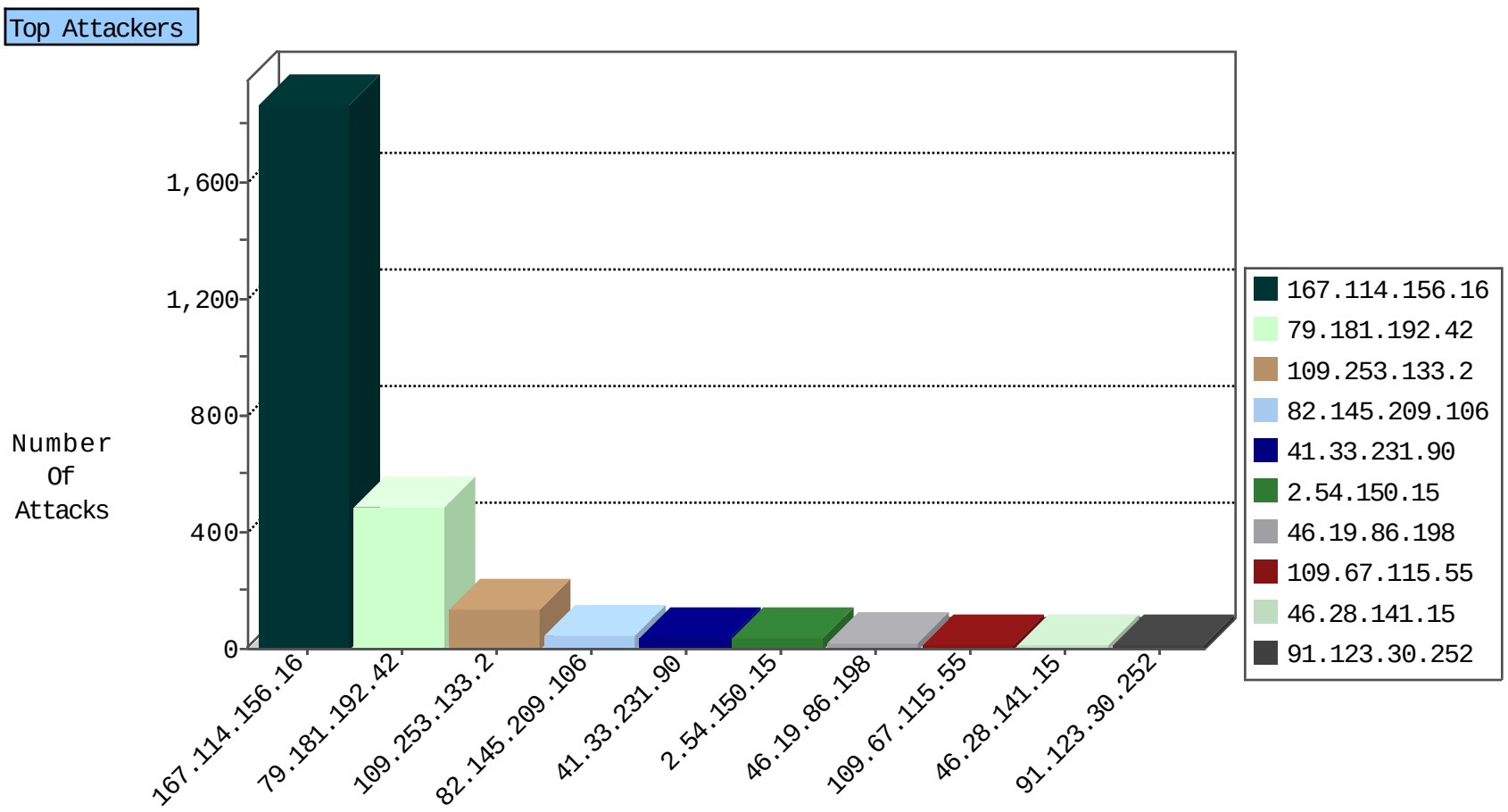
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

12-26-2015-14:04:04 to 12-26-2015-15:04:04

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	3072
172.98.67.112		147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1

12-26-2015-14:04:04 to 12-26-2015-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.118.11.120	Israel	147.237.76.42	refuah.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1

12-26-2015-14:04:04 to 12-26-2015-15:04:04

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
217.132.123.54	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
197.45.153.74	147.237.72.166	Egypt	aka.idf.il	ET SCAN NMAP -sS window 4096	1
197.45.153.74	147.237.72.166	Egypt	aka.idf.il	ET SCAN NMAP -f -sS	1
187.160.214.128	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.81.255.132	147.237.76.31	Brazil	nakchal.idf.il	ET SCAN Potential SSH Scan	1
177.81.255.132	147.237.0.16	Brazil	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
31.19.116.8	147.237.77.235	Germany	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.108.132.58	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
197.45.153.74	147.237.72.166	Egypt	aka.idf.il	ET SCAN NMAP -sS window 2048	1
179.33.11.22	147.237.8.28	Colombia	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.81.255.132	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
31.19.116.8	147.237.77.216	Germany	dover.idf.il	ET SCAN NMAP -sS window 1024	1
218.108.132.58	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

12-26-2015-14:04:04 to 12-26-2015-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.145.209.106	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	46
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.85.82	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
91.123.30.252	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	12
46.28.141.15	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
79.181.192.42	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.64.140.87	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.164.93.91	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
176.12.143.89	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.67.115.55	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
91.78.4.50	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.86.198	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.177.210.163	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
5.102.254.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.29.151.76	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
5.102.254.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.57.132.114	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
213.57.132.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
178.140.107.218	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
188.120.148.131	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.25.203	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.67.135.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
130.193.50.1	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.86.198	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
91.218.150.140	Netherlands	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.28.141.15	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.178.71.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.166.130	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.181.11.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
185.120.125.51		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.49.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
23.254.243.147	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
109.65.12.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.198	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.26	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.104.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.15.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.218.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-26-2015-14:04:04 to 12-26-2015-15:04:04

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.181.141.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.64.166.130	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2

12-26-2015-14:04:04 to 12-26-2015-15:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.192.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	352
79.181.192.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
109.253.133.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
2.54.150.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
109.253.133.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	33
79.181.192.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	18
185.120.125.27		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
37.142.68.87	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	4
37.142.68.87	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	4
176.12.143.89	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
84.109.72.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.166.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
23.254.243.147	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
46.117.124.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.11.217	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
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	2
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
46.166.186.204	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
192.118.11.120	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1440-he/atal.aspx	Block	1
37.142.200.139	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl59 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
86.151.8.155	United Kingdom	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Name	Block	1
79.180.117.66	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
91.185.208.141	Slovenia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.117.124.175	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
184.105.139.70	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
173.252.75.115	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.63.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
74.208.105.30	United States	147.237.72.156	aman.idf.il	E-mail collector robots 14	Block	1
193.201.227.21	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
93.173.190.34	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 93.173.190.34	Block	1
50.116.117.183	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.19.85.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.1.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
86.151.8.155	United Kingdom	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method Â,[[#0]][[#0]][[#0]][[#19]]Ã±[Ã‰Ã™Ã?`Â¿Âª Â?Â¾ÂŸHfÃ”6[[#16]][[#7]]Â?Â¹,Ãƒ Ã‚Ã—ÃµSSÂ,6Ã€[[#30]]Â©Â'[[#25]]Âª Â±VcKÂ¼Ã¼Â•Ã‹[[#16]]Â-Â½-$Lur8Ã¹Â²!Ã'Ãœ Âƒ:[[#1]]Ã„%Â?[[#12]]Ã§[[#28]]Â?qÃ«Ã°Â?[[#29]]Â“Â?ÃŠÃ½Ãº[[#2]]Ãœ[[#25]]	Block	1
79.181.104.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
111.235.136.184	Singapore	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.178.236.154	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	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
91.185.208.141	Slovenia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
46.120.120.188	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
185.52.27.92	United Kingdom	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
173.254.55.58	United States	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
84.109.240.171	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
109.67.115.55	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
74.208.105.30	United States	147.237.72.156	aman.idf.il	eMail Hoarding	Block	1

12-26-2015-14:04:04 to 12-26-2015-15:04:04