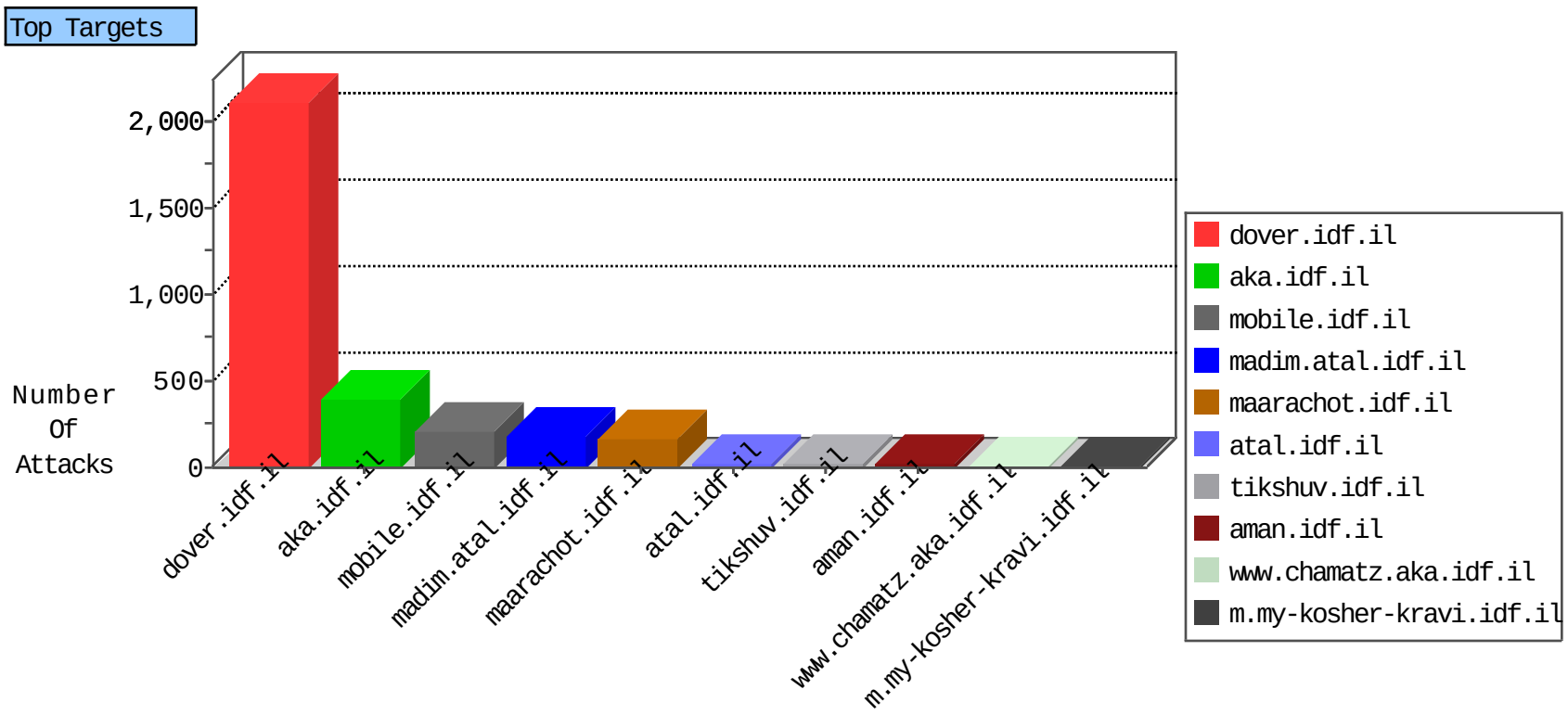
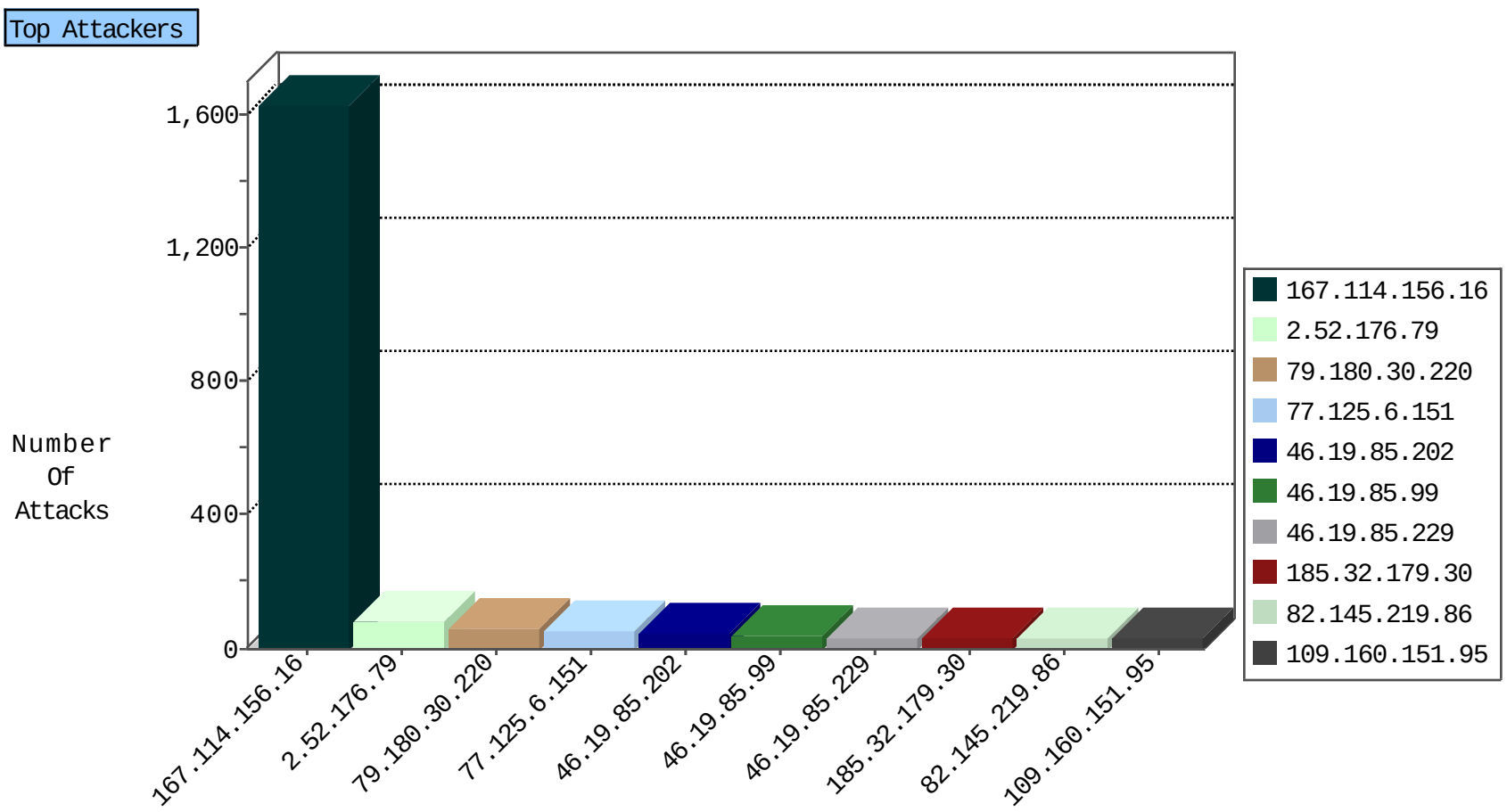
01-03-2016-22:04:03 to 01-03-2016-23:04:03

IDF Under Attack Daily Report



Top Target



Top Attackers

01-03-2016-22:04:03 to 01-03-2016-23:04:03

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	3150
79.183.69.132	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
223.14.15.239	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
77.247.178.132	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1

01-03-2016-22:04:03 to 01-03-2016-23:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-03-2016-22:04:03 to 01-03-2016-23:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.i	Tehila - Perl LWP with fake user agent	12
195.34.150.18	147.237.77.216	Austria	dover.idf.i	Tehila - Perl LWP with fake user agent	4
66.249.78.172	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
66.249.78.160	147.237.72.166	United States	aka.idf.il	WEB-CGI redirect access	1

01-03-2016-22:04:03 to 01-03-2016-23:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.125.6.151	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
46.19.85.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
82.145.219.86	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	30
85.130.224.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
77.127.233.192	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
2.52.176.79	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	20
5.29.75.205	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
46.19.85.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
77.127.24.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.121.37.28	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
2.52.176.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
2.52.176.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.85.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
2.52.176.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	15
46.19.85.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.10	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.253.210.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
99.38.63.6	United States	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
37.26.148.185	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	13
176.12.150.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
79.179.120.43	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
95.90.246.52	Germany	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
2.52.176.79	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
5.28.139.94	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
46.19.86.146	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
109.67.183.181	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
5.28.181.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.3.144.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
31.210.187.62	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
84.108.62.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
46.120.130.11	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.86.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.229	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.19	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.228.8.62	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
167.160.116.202	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
217.132.135.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.170.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.229	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6

01-03-2016-22:04:03 to 01-03-2016-23:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.30.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
46.19.85.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
176.12.141.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.85.202	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.210.83	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
185.32.179.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.19.86.10	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
94.159.146.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
94.159.146.15	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	3
109.160.151.95	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
77.125.129.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.146.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.10.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.183.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.131	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.196.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.27.105.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.68.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.28.181.88	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.160.151.95	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 109.160.151.95	Block	2
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	2
109.160.151.95	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 109.160.151.95	Block	2
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	2
2.52.35.54	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
95.35.171.87	Israel	147.237.0.17	m.my-kosher-kravi .idf.il	Distributed Illegal Parameter Encoding	None	2
109.253.150.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.228.8.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.160.151.95	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 109.160.151.95	Block	2
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	2
109.160.151.95	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 109.160.151.95	Block	2
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	2
149.78.41.185	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.117.113.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.160.151.95	Israel	147.237.72.166	aka.idf.il	NULL Character in Method RnÃ¢Â—Â¢Â¥[[#8]]Ã¾WÃ˜Â‹Ã±Â–Â…dÂ?Â› ÃªlÃ¸ :Â?[[#27]][[[#30]]$HÂŒÂ›[[#26]]Â³[[#30]]Ã‰•[[#0]]Â?[[#27]]Ã‰ [[#14]]AEÂ-Â†Âª[[#31]]Â§Âš\GÃµÃ°8ÂŽÂ‹Â¯Â–ÃŒfÂ»Ã?Â?Â˜ Â²Ã©Ã¹<RyÂ·P2Â?Ã’	Block	1
85.250.89.88	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
50.148.136.177	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.160.151.95	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method RnÃ¢Â—Â¢Â¥[[#8]]Ã¾WÃ˜Â‹Ã±Â–Â…dÂ?Â›Ãªlã¸ :Â?[[#27]][[[#30]]$HÂŒÂ›[[#26]]Â³[[#30]]Ã‰ •[[#0]]Â?[[#27]]Ã‰[[#14]]AEÂ-Â†Âª[[#31]]Â§Âš\GÃµÃ°8ÂŽÂ‹Â¯Â–ÃŒ fÂ»Ã?Â?Â˜Â²Ã©Ã¹<RyÂ·P2Â?Ã’	Block	1
79.182.110.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.127.176.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.195.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	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
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.160.151.95	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method RnÃ¢Â—Â¢Â¥[[#8]]Ã¾WÃ˜Â‹Ã±Â–Â… dÂ?Â›Ãªlã¸ :Â?[[#27]][[[#30]]$HÂŒÂ›[[#26]]Â³[[#30]]Ã‰ •[[#0]]Â?[[#27]]Ã‰[[#14]]AEÂ-Â†Âª[[#31]]Â§Âš\GÃµÃ°8ÂŽÂ‹Â¯Â–ÃŒ fÂ»Ã?Â?Â˜Â²Ã©Ã¹<RyÂ·P2Â?Ã’ in URL Â 6tÃ™ qm[[#15]]×¤[[#21]][[#29]]jrqÃœ[[#23]]ÃŸ!ÃŸ×‘×¦ÃŸrÖ¼ÂŸo	Block	1
31.44.134.36	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.44.134.36	Block	1
2.54.142.254	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
84.108.174.179	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	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

01-03-2016-22:04:03 to 01-03-2016-23:04:03