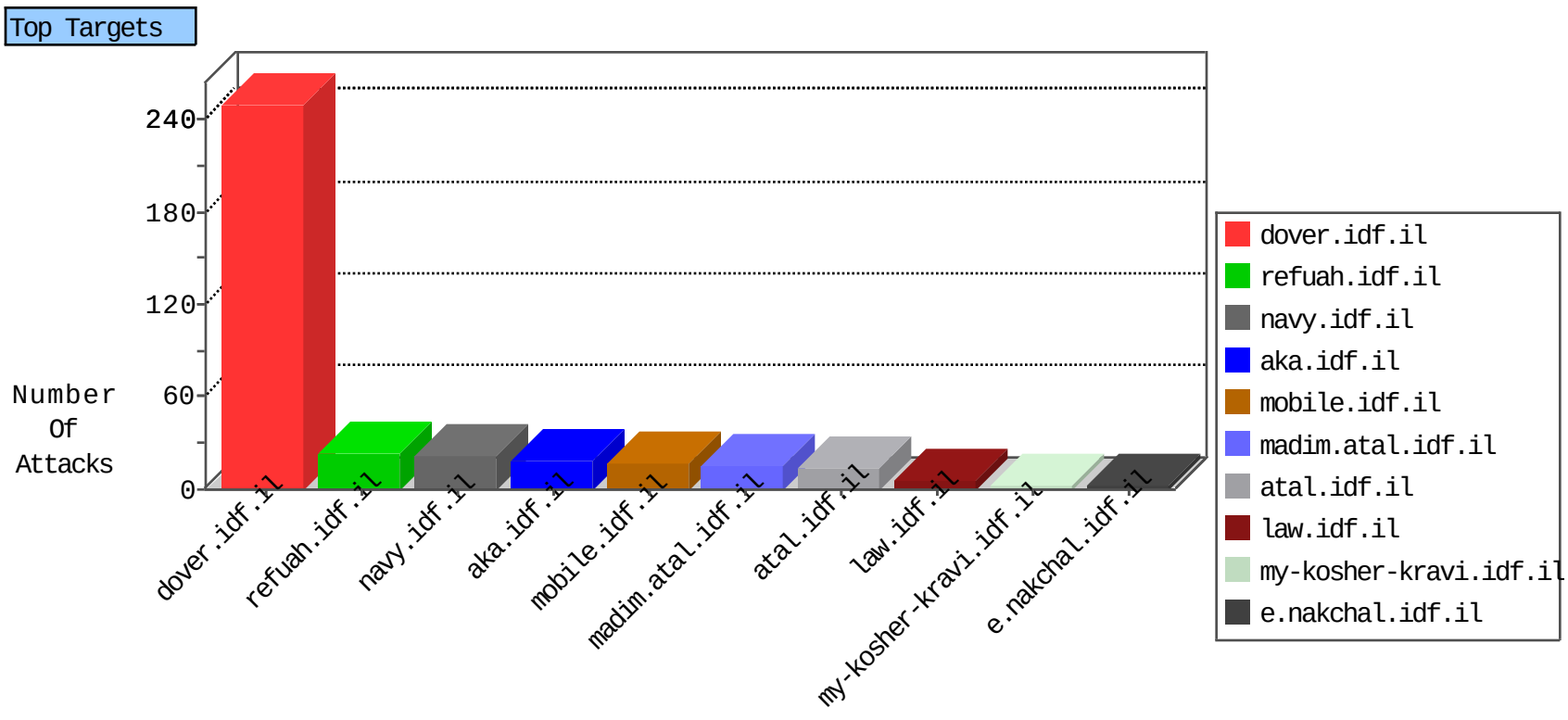
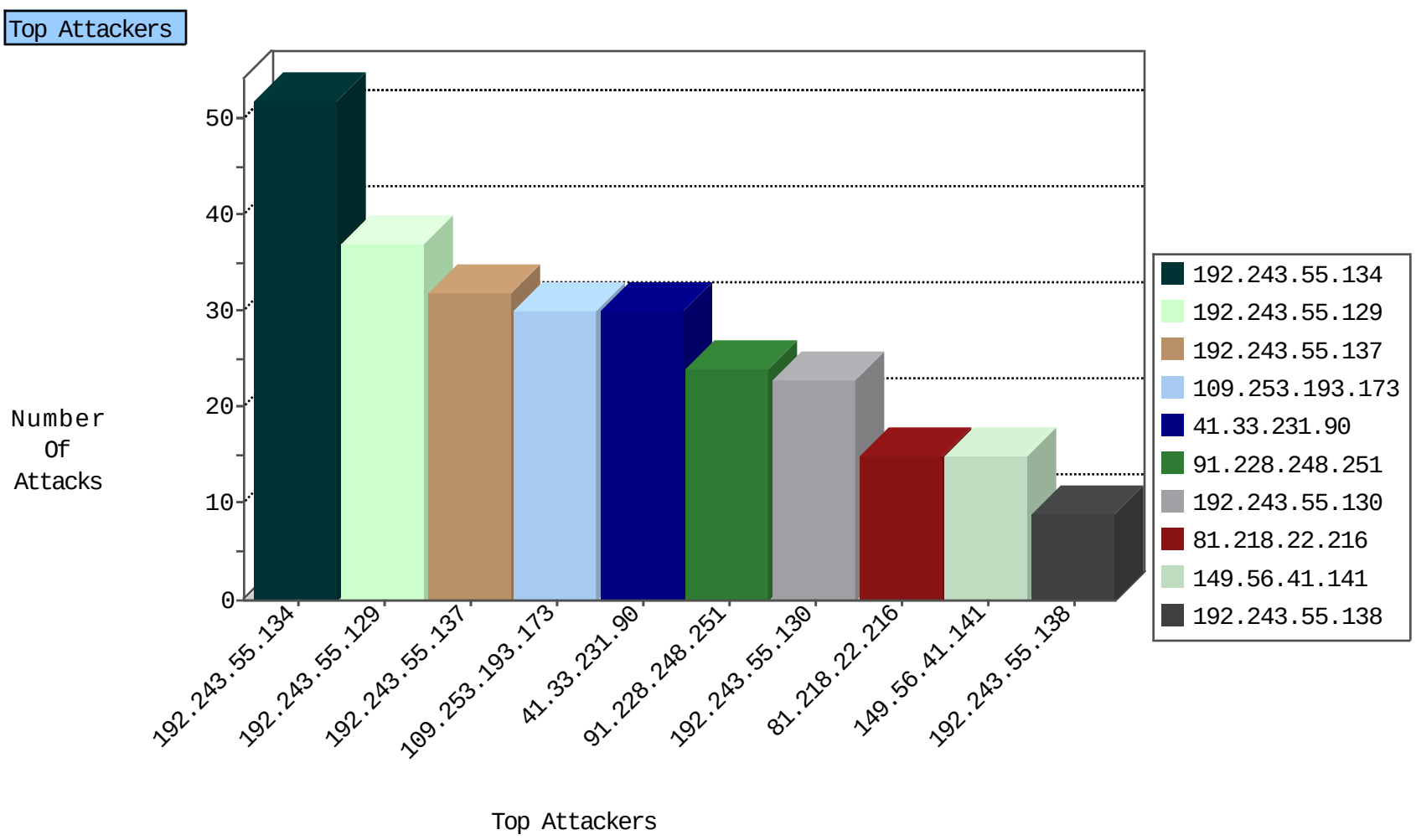
02-21-2016-04:04:02 to 02-21-2016-05:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-21-2016-04:04:02 to 02-21-2016-05:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
115.239.228.10	China	147.237.76.31	nakchal.idf.il	JLM_Under_Attack_Con_Http	drop	2
185.130.5.174		147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.174		147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.174		147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1

02-21-2016-04:04:02 to 02-21-2016-05:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.228.248.251	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
149.56.41.141	United States	147.237.72.166	aka.idf.il	C1000023: HTTP: administrator in URI	Block	1

02-21-2016-04:04:02 to 02-21-2016-05:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
81.218.22.216	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
149.56.41.141	147.237.72.166	United States	aka.idf.il	SERVER-WEBAPP admin.php access	1
146.185.250.2	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
146.185.250.2	147.237.76.201	Russian Federation	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
104.215.89.20	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
61.143.38.96	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

02-21-2016-04:04:02 to 02-21-2016-05:04:02

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	30
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
109.253.193.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.137	Dominica	147.237.77.216	dover.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	8
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
123.103.8.95	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.74.9	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.74.12	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.137	Dominica	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
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
81.218.22.216	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
185.32.179.136	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
123.103.8.95	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.180.235.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
66.249.74.6	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
81.218.22.216	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
81.218.22.216	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
45.55.53.138		147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
184.105.247.236	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.72	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.124	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.172.193.32	Hungary	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1

02-21-2016-04:04:02 to 02-21-2016-05:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.193.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
134.249.54.139	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	6
149.56.41.141	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.56.41.141	Block	5
149.56.41.141	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	4
149.56.41.141	United States	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 149.56.41.141	Block	3
109.253.193.173	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	2
24.216.73.76	United States	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
209.95.50.12	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
24.216.73.76	United States	147.237.76.86	navy.idf.il	Unknown HTTP Request Method Â,[[#0]][[#0]][[#0]]!lAâ€Â•?UÃ€Ã‘ &J}^rÃ–Ã´Â«[Â²Ã¤+[[#0]]Ã·Â¥4qÂ¼Â–Â™[[#28]][[#15]]Â•Â?Ã·ÂŸ Ã¿Â”Â?;Ã–Â»ÃˆÂˆÂ˜ in URL dÂ±[[#27]]"Â?×£Â½â€°Ö¶Â´×š [[#1]]×¦u[[#16]]hÂŒi6zÂ¡![[#4]]Â¨×±5Â?Â¿[[#23]]ÂžÂµ×ž×˜[[#31]]â€ ¦Ã™×'Â-×•Â´z[[#14]][[#8]]Ã–â€¹[k^l•Ã¼Ö¹q×£Â·ÃŠ-qcË†×' pn6Â¼[[#28]]Â»v<va	Block	1
149.202.74.134	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
83.149.37.79	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
24.216.73.76	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method Â,[[#0]][[#0]][[#0]]!lAâ€Â•?UÃ€ Ã'&J}^rÃ–Ã´Â«[Â²Ã¤+[[#0]]Ã·Â¥4qÂ¼Â–Â™[[#28]][[#15]]Â•Â?Ã·ÂŸ Ã¿Â”Â?;Ã–Â»ÃˆÂˆÂ˜	Block	1
213.147.108.22	Croatia	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
40.77.167.57	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
157.55.39.146	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
83.149.37.79	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
24.216.73.76	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in URL dÂ±[[#27]]"Â?×£Â½â€°Ö¶Â´×š [[#1]]×¦u[[#16]]hÂŒi6zÂ¡![[#4]]Â¨×±5Â?Â¿[[#23]]ÂžÂµ×ž×˜[[#31]]â€ ¦Ã™×'Â-×•Â´z[[#14]][[#8]]Ã–â€¹[k^l•Ã¼Ö¹q×£Â·ÃŠ-qcË†×' pn6Â¼[[#28]]Â»v<va	Block	1
213.147.108.22	Croatia	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/wp-login.php	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
184.105.139.70	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
24.216.73.76	United States	147.237.76.86	navy.idf.il	Malformed URL dÂ±[[#27]]"Â?×£Â½â€°Ö¶Â´×š[[#1]]×¦u[[#16]]hÂŒ i6zÂ¡![[#4]]Â¨×±5Â?Â¿[[#23]]ÂžÂµ×ž×˜[[#31]]â€¦Ã™×'Â-×• Â´z[[#14]][[#8]]Ã–â€¹[k^l•Ã¼Ö¹q×£Â·ÃŠ-qcË†×'pn6Â¼[[#28]]Â»v<va	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/idf_in_pictures/2002/april/	Block	1
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0113-3.stm`	Block	1
24.216.73.76	United States	147.237.76.86	navy.idf.il	NULL Character in Method Â,[[#0]][[#0]][[#0]]!lAâ€Â•?UÃ€Ã'&J}^rÃ– Ã´Â«[Â²Ã¤+[[#0]]Ã·Â¥4qÂ¼Â–Â™[[#28]][[#15]]Â•Â?Ã·ÂŸÃ¿Â”Â?;Ã– Â»ÃˆÂˆÂ˜	Block	1
149.56.41.141	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
79.181.115.176	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1

02-21-2016-04:04:02 to 02-21-2016-05:04:02