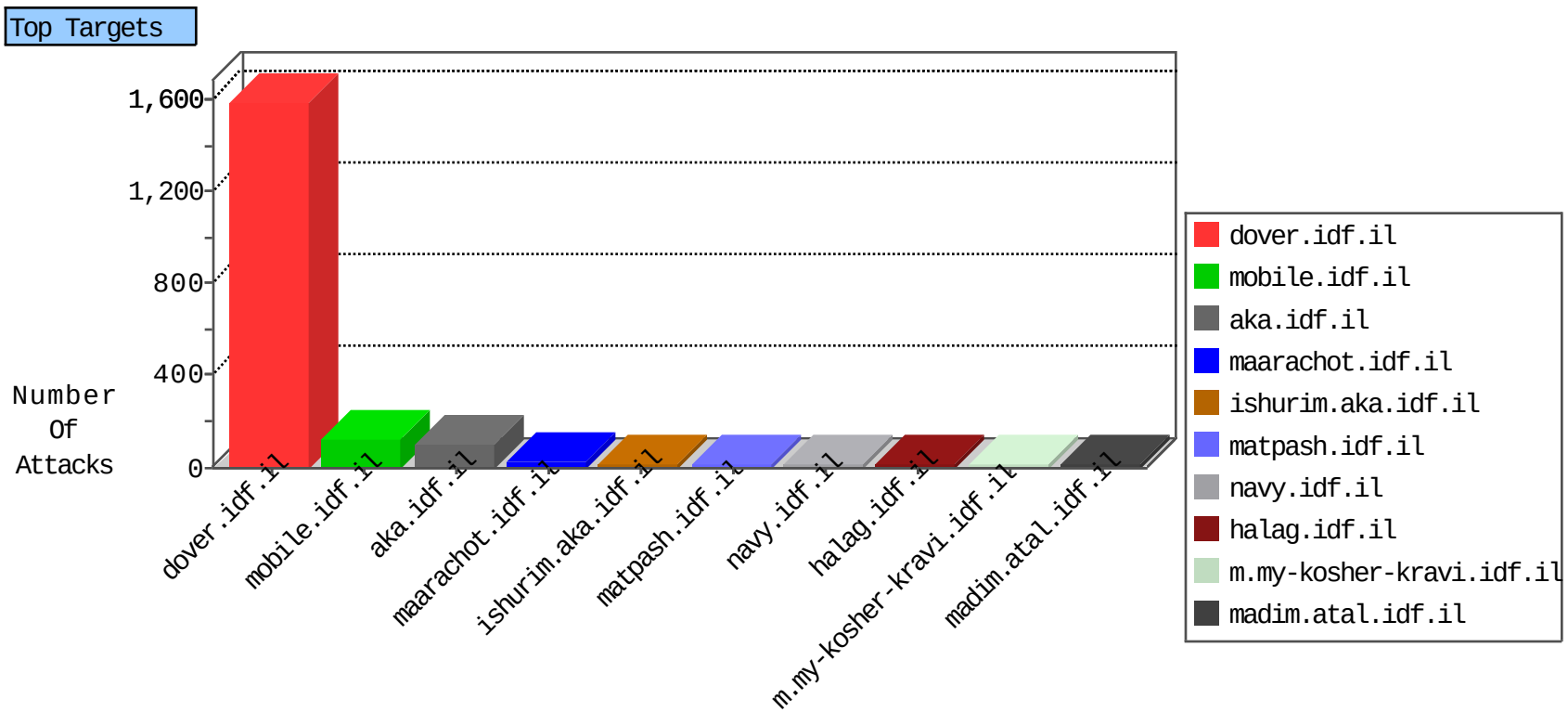
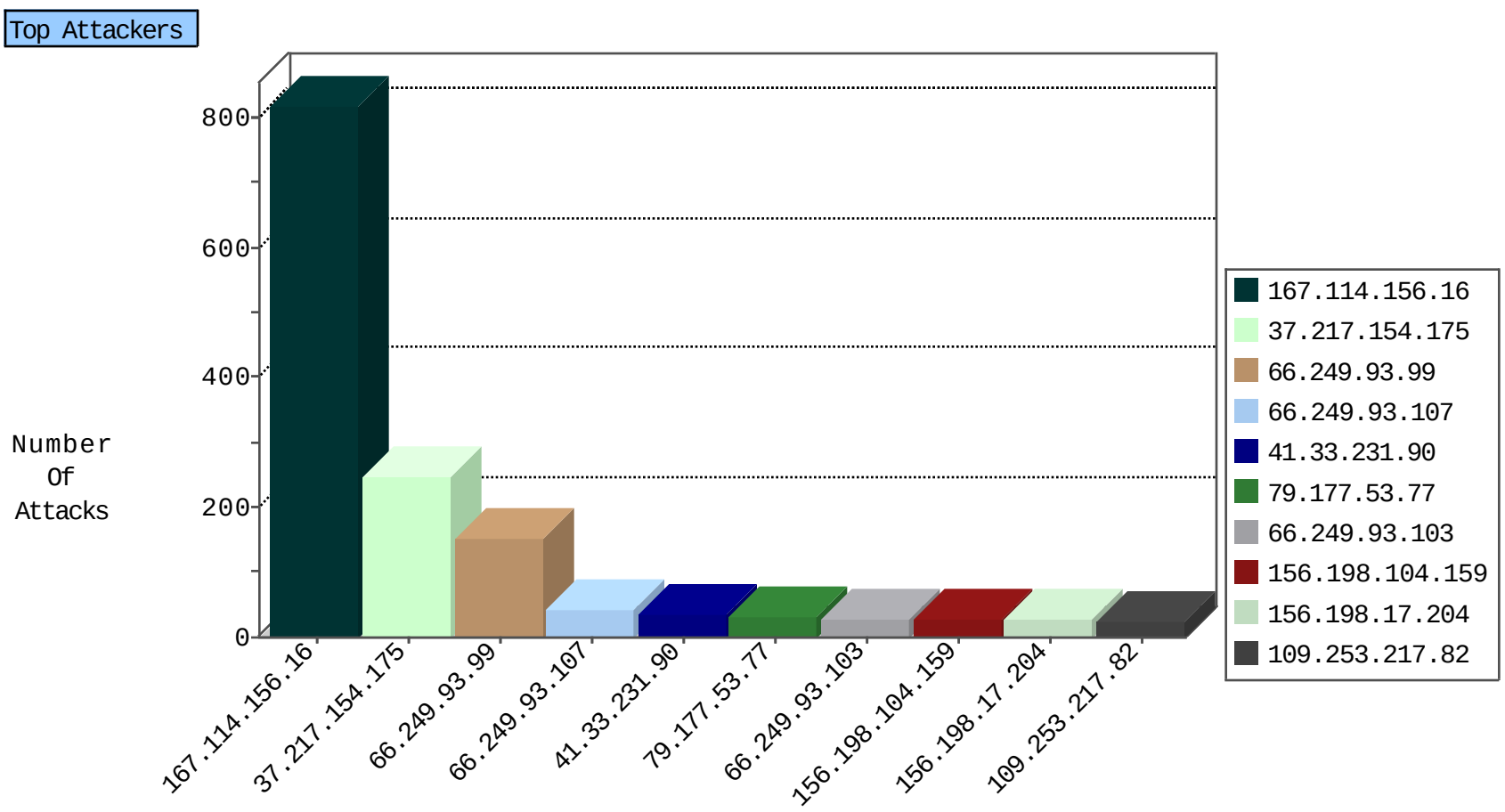
01-01-2016-00:04:02 to 01-01-2016-01:04:02

IDF Under Attack Daily Report



Top Target



Top Attackers

01-01-2016-00:04:02 to 01-01-2016-01:04:02

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	3015
109.64.4.233	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
66.249.93.107	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
108.6.31.115	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
157.55.81.9	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

01-01-2016-00:04:02 to 01-01-2016-01:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.40.45.254	Egypt	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	3
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
212.48.68.50	United Kingdom	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

01-01-2016-00:04:02 to 01-01-2016-01:04:02

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	4
197.40.45.254	147.237.77.216	Egypt	dover.idf.il	GPL WEB_SERVER /etc/passwd	3
197.40.45.254	147.237.77.216	Egypt	dover.idf.il	SQL Injection - Select From	3
66.249.66.23	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
192.198.216.130	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
183.82.106.200	147.237.76.42	India	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
40.122.124.70	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
183.82.106.200	147.237.76.42	India	refuah.idf.il	ET SCAN NMAP -f -sS	1
40.122.124.70	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.238	147.237.76.176		test.ncore.idf.il	ET SCAN NMAP -f -sS	1
108.61.190.137	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 3072	1
104.143.14.247	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
208.67.1.155	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.191.221	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
192.198.216.130	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
192.198.216.130	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
183.82.106.200	147.237.76.42	India	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
40.122.124.70	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.238	147.237.76.176		test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
40.122.124.70	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
108.61.190.137	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
208.67.1.155	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.77.121		e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.78.158	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

01-01-2016-00:04:02 to 01-01-2016-01:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.217.154.175	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	122
37.217.154.175	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	119
66.249.93.99	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	50
66.249.93.99	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	50
66.249.93.99	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
213.175.160.22	Lebanon	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
2.52.8.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.93.107	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
66.249.93.107	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	11
46.19.86.209	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
156.198.17.204		147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
66.249.66.48	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
79.177.63.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.209	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
66.249.66.63	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
156.198.104.159		147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.149.149	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.180.155.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.107	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.117.102.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.103	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	6
82.80.143.207	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
66.249.93.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.103	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.93.103	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.185	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
89.138.23.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.64.124.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.4	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.253.197.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
85.65.26.61	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
130.193.51.64	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
5.102.254.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.22.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.36	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.65.23.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.44		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-01-2016-00:04:02 to 01-01-2016-01:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.53.77	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	29
109.253.217.82	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	21
79.180.102.69	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	9
46.19.85.201	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
37.105.197.203	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/'	Block	3
197.40.45.254	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.40.45.254	Block	3
37.26.148.237	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	3
156.198.104.159		147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	2
109.253.217.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.174.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
156.198.38.225		147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
156.198.104.159		147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	2
2.52.8.160	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.180.48.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
156.198.104.159		147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	2
156.198.104.159		147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	2
156.198.38.225		147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	2
2.52.149.143	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.12.149.35	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	2
85.250.137.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
156.198.104.159		147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
156.198.38.225		147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
156.198.38.225		147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	2
156.198.104.159		147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	2
156.198.103.235		147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
149.88.51.179	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	2
37.60.47.212	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.60.47.212	Block	2
2.54.33.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
156.198.38.225		147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	2
79.182.187.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.151.149	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	2
156.198.38.225		147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	2
79.177.53.77	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	2
156.198.17.204		147.237.77.216	dover.idf.il	Illegal Byte Code Character in Parameter Value at 10 for Â¨[[#15]]×›â„¢a×€$qz2×£×œÂ«[[#11]]r[[#23]]1cyâ,ª>×,•a"+ Ö»×?â€¦Ö´"Â£[[#6]]!â„¢Â-×?[[#12]]%z	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
156.198.103.235		147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
213.61.149.100	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
85.64.124.107	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.120.125.60		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
156.198.104.159		147.237.77.216	dover.idf.il	Malformed HTTP Header Line 4	Block	1
156.198.17.204		147.237.77.216	dover.idf.il	Malformed URL Â¨[[#15]]×›â„¢a×€$qz2×£×œÂ«[[#11]]r[[#23]]1cyâ,ª>×,•a"+ Ö»×?â€¦Ö´"Â£[[#6]]!â„¢Â-×?[[#12]]%z	Block	1
46.117.102.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
156.198.17.204		147.237.77.216	dover.idf.il	Abnormally Long Request request version	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
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
156.198.38.225		147.237.77.216	dover.idf.il	Distributed NULL Character in Header Name	Block	1
156.198.17.204		147.237.77.216	dover.idf.il	Unknown HTTP Request Method vGÂ¹QÂ¦:GÃ·Ã¡Â°IcjÃ¡()[[#19]]Ã,Ã… H[[#25]]ÂšÂ'Â·Ã¾Ã¥Ã¯Ã¨[[#16]][[#0]][[#8]]{Ã¦[[#4]]Â¡Â‡7Ã£3Â″Ãš CÂ–Ã–yÃ«[[#27]]Â¨ÂªÃ»Ã¨Ã?KÃ‰mÂ¥Ã§{Â?Ã¶[[#17]]Ã¹U@Ã‡	Block	1
156.199.6.40		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1

01-01-2016-00:04:02 to 01-01-2016-01:04:02