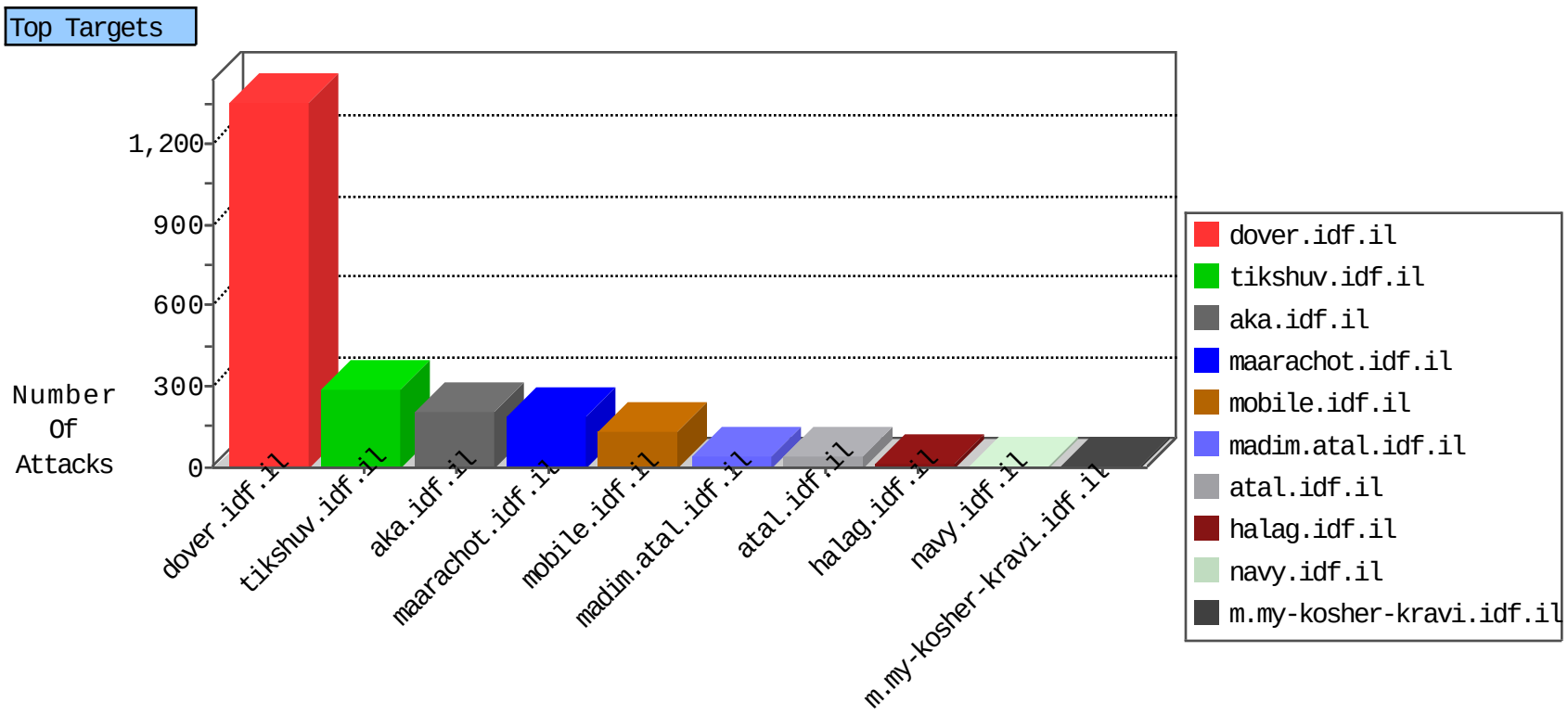
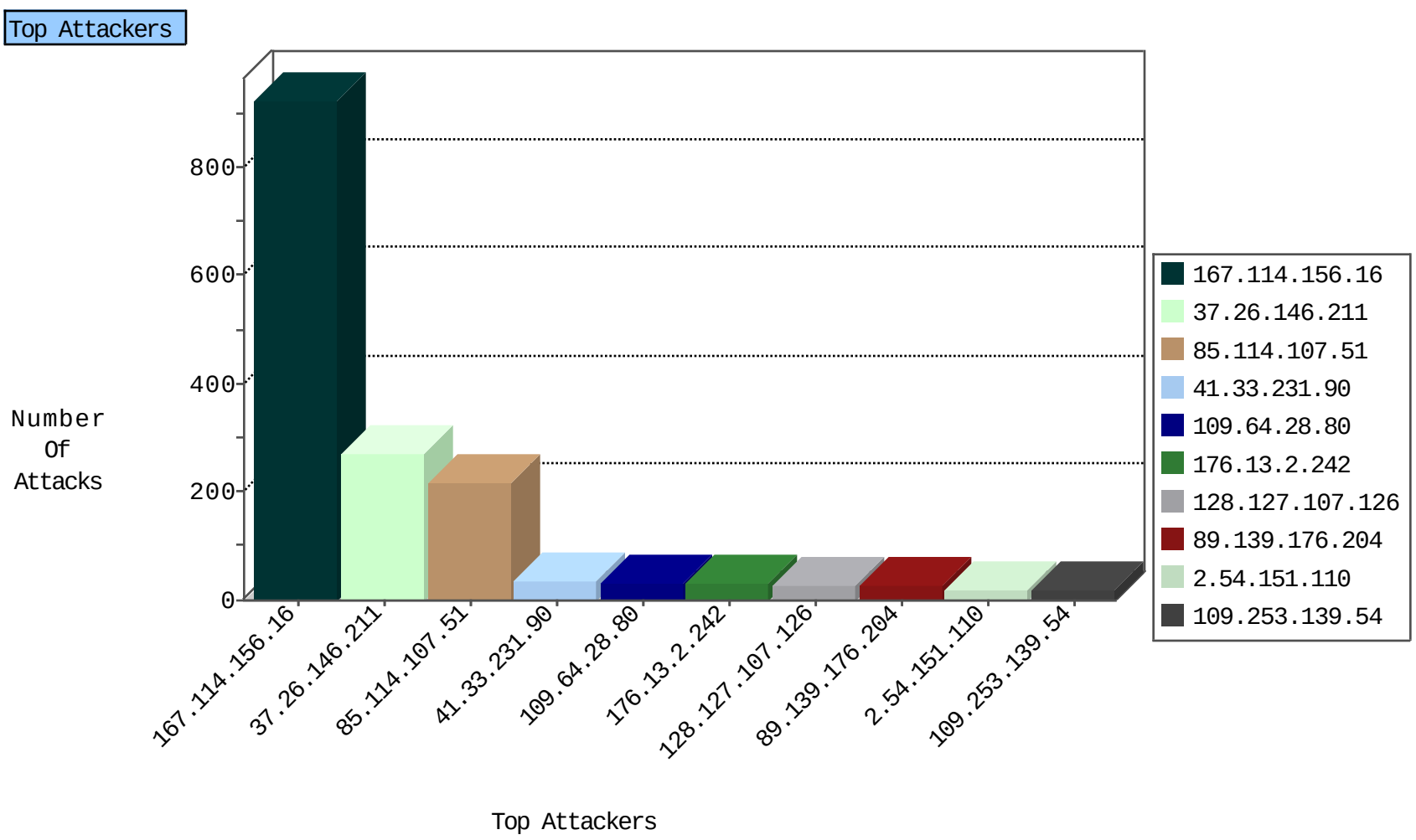
01-01-2016-16:04:03 to 01-01-2016-17:04:03

IDF Under Attack
Daily Report



Top Target



Top Attackers

01-01-2016-16:04:03 to 01-01-2016-17:04:03

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	3023
85.114.107.51	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP-MISC-Havij-User-Agent	dest-reset	186
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
141.212.122.123	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.124	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

01-01-2016-16:04:03 to 01-01-2016-17:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-01-2016-16:04:03 to 01-01-2016-17:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.151.110	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
172.98.200.238	147.237.72.14		dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
189.63.32.161	147.237.77.235	Brazil	sviva.idf.il	ET SCAN Potential SSH Scan	1
122.96.50.223	147.237.72.14	China	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
189.63.32.161	147.237.77.227	Brazil	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
93.189.26.18	147.237.76.202	Austria	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
189.63.32.161	147.237.77.205	Brazil	prisha.idf.il	ET SCAN Potential SSH Scan	1
80.246.133.37	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
189.63.32.161	147.237.77.170	Brazil	maarachot.idf.il	ET SCAN Potential SSH Scan	1
189.63.32.161	147.237.77.19	Brazil	law-forum.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.235	147.237.0.19		madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.235	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
192.186.95.178	147.237.76.39	Canada	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.238	147.237.72.14		dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
192.81.13.19	147.237.0.34	Canada	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.238	147.237.72.14		dover.idf.il(old)	ET SCAN NMAP -f -sS	1
189.63.32.161	147.237.77.234	Brazil	halag.idf.il	ET SCAN Potential SSH Scan	1
106.75.199.173	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
189.63.32.161	147.237.77.212	Brazil	e.dover.idf.il	ET SCAN Potential SSH Scan	1
93.189.26.18	147.237.76.44	Austria	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
189.63.32.161	147.237.77.178	Brazil	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
27.204.162.144	147.237.8.45	China	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
189.63.32.161	147.237.77.61	Brazil	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.235	147.237.0.35		akaws.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.235	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
192.186.95.178	147.237.76.39	Canada	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
177.229.129.237	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
192.81.13.19	147.237.0.34	Canada	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1

01-01-2016-16:04:03 to 01-01-2016-17:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.146.211	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	271
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
109.64.28.80	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
85.114.107.51	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	27
89.139.176.204	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
128.127.107.126	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	21
109.253.139.54	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.183.175.131	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
176.13.2.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
79.183.152.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.180.175.70	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
66.249.66.48	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.176.96.42	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
109.64.121.68	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
46.19.85.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.78.245.104	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
94.159.158.225	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
87.68.243.92	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
2.54.151.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.180.175.27	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
149.78.47.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.34.101.209	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.133.153	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
43.255.176.89	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.230.37.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
128.127.107.126	Netherlands	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.173.129.141	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
2.54.187.28	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.45.19	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.183.164.148	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
81.240.125.209	Belgium	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
89.138.10.33	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.51	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
77.125.102.42	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
93.173.129.141	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	4
109.64.110.175	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
79.180.120.92	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
52.6.67.132	United States	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
79.181.146.152	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
176.13.20.27	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.182.49.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.159.170.206	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
5.102.253.0	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

01-01-2016-16:04:03 to 01-01-2016-17:04:03

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
84.229.35.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-01-2016-16:04:03 to 01-01-2016-17:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.228.12.229	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 176.228.12.229	Block	9
79.182.193.222	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	8
176.13.2.242	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	7
176.13.2.242	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
79.182.193.222	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.182.193.222	Block	6
176.13.4.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.187.28	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	5
94.230.83.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.54.187.28	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.195.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.68.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
207.46.13.144	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.144	Block	3
46.19.85.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.139	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
84.229.35.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.191	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
79.181.55.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
46.19.85.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.102.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.135.75	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 109.253.135.75	None	2
149.78.39.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.133.37	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
212.199.107.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.129.242	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.180.8.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	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
2.54.177.91	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
104.199.141.224	United States	147.237.77.216	dover.idf.il	Multiple Malformed URL from 104.199.141.224	Block	1
93.173.231.46	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9067-he/refuah.aspx	Block	1
46.19.86.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.147.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.47.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
208.117.46.253	United States	147.237.72.166	aka.idf.il	Unknown Parameter author in www.aka.idf.il/	None	1
79.176.50.225	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on 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
104.199.141.224	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method [[#0]][[#0]][[#6]][[#4]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#4]]@[[#0]][[#0]][[#0]][[#0]][[#0]][[#8]][[#6]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#4]][[#8]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[0]]@[[#0]][[#0]][[#0]][[#0]][[#0]]&[[#1]]%[[#0]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]]Â,Â„Â‡AÂˆÃ±Ã£Ã,Ã¦Â'UÃ?GS[[#3]]*/*zÂ?Âªià'ÂšÃ„Ã€ WmpÂ-•[[#7]][[#31]][[#0]][[#0]][[#11]][[#1]]%[[#0]][[#0]][[#0]][[#3]][[#0]][[#0]][[#0]][[#1]]	Block	1
66.249.66.90	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/	Block	1
149.78.47.198	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.228.168.204	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH)	None	1
80.246.136.71	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
213.57.43.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.186.30.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
104.199.141.224	United States	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 104.199.141.224	Block	1
79.180.190.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-01-2016-16:04:03 to 01-01-2016-17:04:03