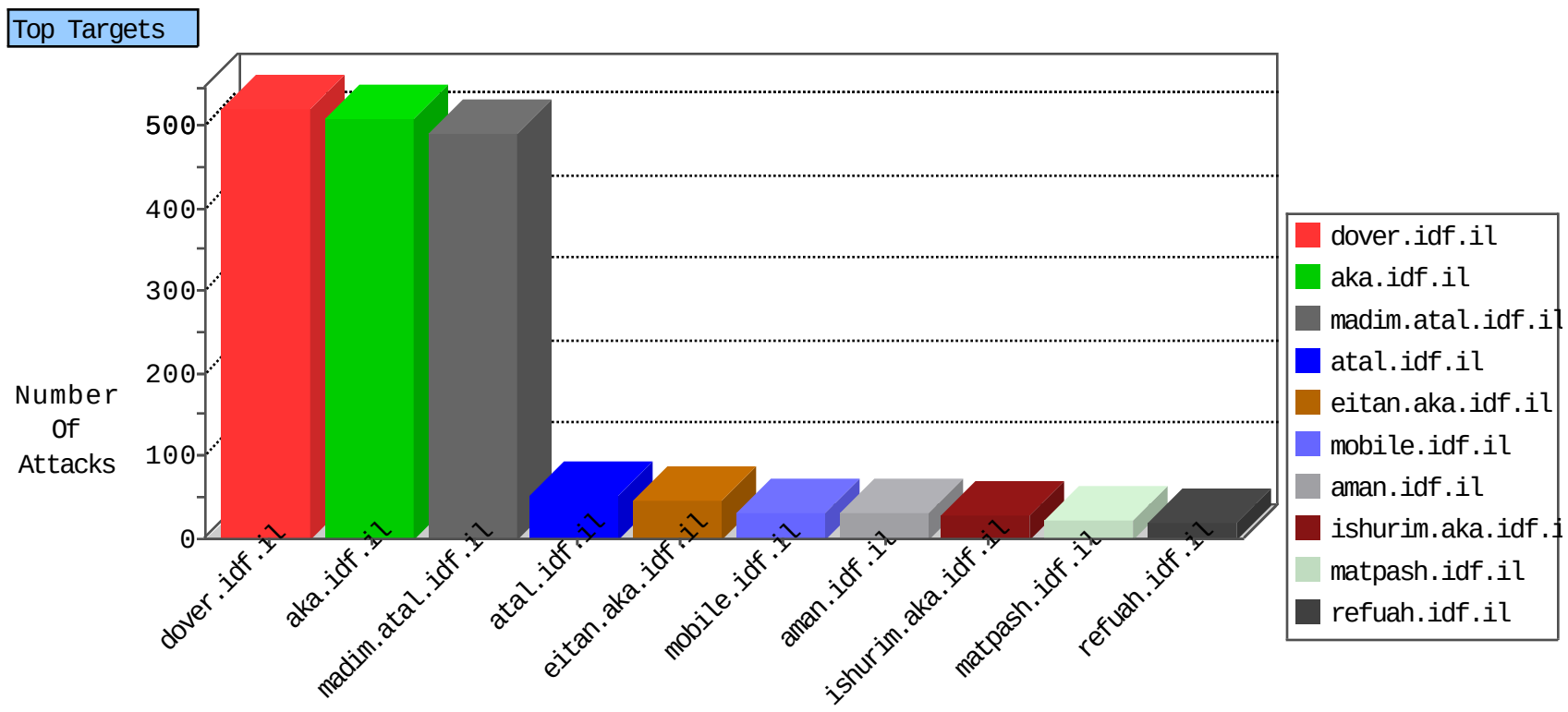
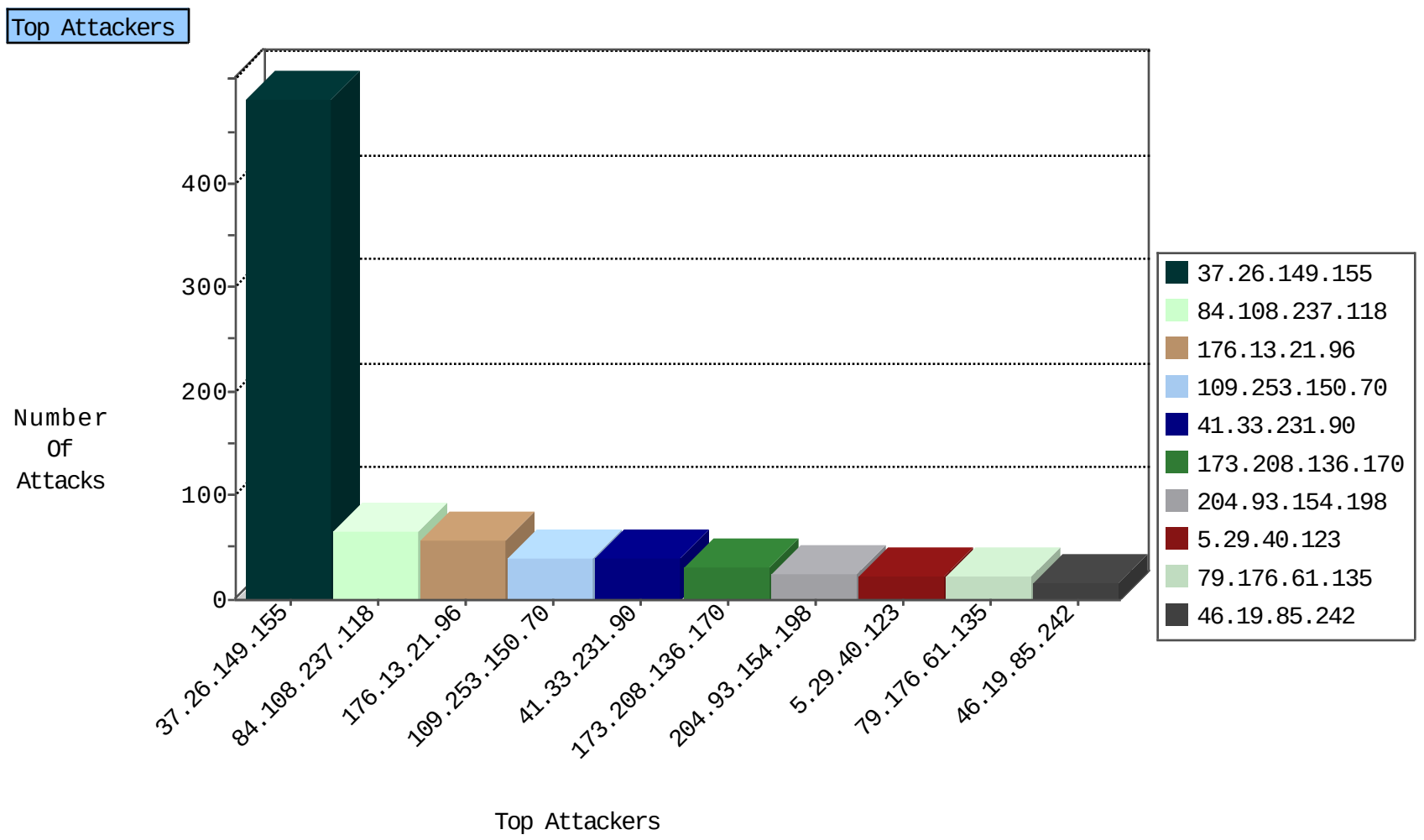
02-21-2016-21:04:00 to 02-21-2016-22:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-21-2016-21:04:00 to 02-21-2016-22:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.154.198	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	195
5.196.80.160	France	147.237.77.233	atal.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
134.147.203.115	Germany	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	2
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
198.20.70.114	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.123	Switzerland	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

02-21-2016-21:04:00 to 02-21-2016-22:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.137.1	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
5.196.80.160	France	147.237.77.233	atal.idf.il	10767: HTTP: Acunetix Security Scanner	Block	4
106.120.173.109	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
109.67.107.142	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
151.80.41.169	Italy	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
40.77.167.71	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
157.55.39.97	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

02-21-2016-21:04:00 to 02-21-2016-22:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
2.54.60.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.223.25.134	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN NMAP -sS window 1024	1
87.70.24.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.38.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.230.55.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.155	147.237.0.19	Israel	madim.atal.idf.i	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
203.213.234.118	147.237.76.38	Australia	e.e.meitav.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.29.128.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
189.202.241.84	147.237.77.61	Mexico	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.148.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
105.155.175.116	147.237.76.42	Morocco	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
87.70.55.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.126.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.31.171	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.117.125.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.68.91	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.3.140.45	147.237.72.166	China	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.154.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.76.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.148.254	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-21-2016-21:04:00 to 02-21-2016-22:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.21.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
109.253.150.70	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
173.208.136.170	United States	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	22
79.176.61.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
80.246.136.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.55.82	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
79.178.23.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.59.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.147.235	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.147.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.162.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.31.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
193.106.54.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.12.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.144.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.70.13.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.144.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.193.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.5.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.18.52	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.142.72.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
31.210.187.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.148.96	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

02-21-2016-21:04:00 to 02-21-2016-22:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	344
37.26.149.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	137
84.108.237.118	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.237.118	Block	42
84.108.237.118	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	22
5.29.40.123	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.29.40.123	Block	14
5.29.40.123	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	8
173.208.136.170	United States	147.237.77.233	atal.idf.il	Multiple Admin Blocking from 173.208.136.170	Block	8
109.65.160.208	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/newsarchive.aspx	Block	4
167.114.64.100	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/.	Block	4
46.19.85.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
212.76.109.241	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1337-he/cogat.aspx&sa=u&ved=0ahukewjg5cyryinlahxkipokhcbubx0qfggimaa&usg=afqjcnhfwsegkf4gz3l8cxi3ba2lrpsseq	Block	4
176.13.18.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.106.130	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	3
79.177.106.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	3
46.19.85.94	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	2
84.108.237.118	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	2
212.179.243.156	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
148.251.21.227	Germany	147.237.77.74	law.idf.il	Distributed Suspicious Response Code	Block	2
84.94.88.207	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
66.249.81.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.19.116.75	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	2
212.76.103.173	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.76.103.173	Block	2
109.125.16.115	Ireland	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	2
89.120.94.39	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1395-en/dover.aspx	Block	2
84.111.60.187	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	2
212.179.243.156	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.179.243.156	Block	2
198.20.69.74	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	2
5.28.181.29	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	2
173.208.136.170	United States	147.237.77.233	atal.idf.il	Admin Blocking	Block	2
89.120.94.39	Romania	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-en/cogat.aspx	Block	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	2
89.120.94.39	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1395-en/dover.aspx	Block	2
5.41.140.221	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
85.224.94.139	Sweden	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	2
2.54.59.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.64.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	2
157.55.12.86	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	2
176.116.188.83	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	2
109.65.210.66	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	2
46.19.86.217	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
89.120.94.39	Romania	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/1043-en/cogat.aspx	Block	2
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	2
212.76.109.241	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 212.76.109.241	Block	2
79.177.106.130	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
109.253.210.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.148.196.86	Netherlands	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	2
89.138.109.154	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	2
79.178.152.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	2

02-21-2016-21:04:00 to 02-21-2016-22:04:00