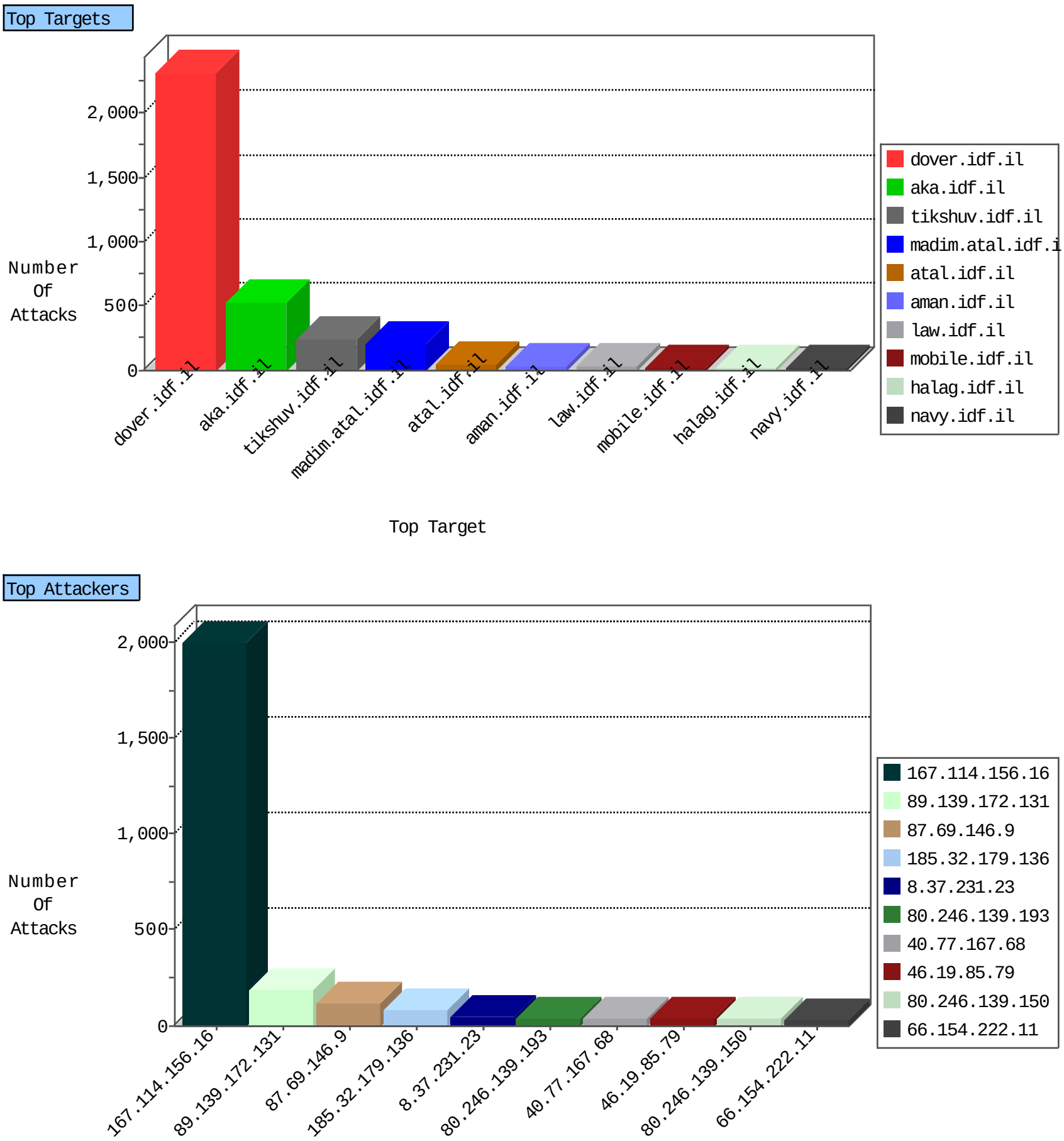
01-12-2016-19:04:01 to 01-12-2016-20:04:01

IDF Under Attack Daily Report



01-12-2016-19:04:01 to 01-12-2016-20:04:01

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	3054
92.19.166.41	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
8.37.231.23	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	1
114.163.87.32	Japan	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

01-12-2016-19:04:01 to 01-12-2016-20:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
88.226.188.201	Turkey	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

01-12-2016-19:04:01 to 01-12-2016-20:04:01

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
79.180.180.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
223.95.76.85	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
61.239.172.2	147.237.76.30	Hong Kong	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.20.69.76	147.237.77.212	United States	e.dover.idf.il	ET DROP Dshield Block Listed Source	1
50.204.188.142	147.237.8.46	United States	e.chinuch.idf.i	ET SCAN NMAP -sS window 2048	1
185.106.92.107	147.237.76.199		e.nakchal.idf.i	ET SCAN NMAP -sS window 1024	1
31.154.253.217	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
158.255.6.220	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
122.224.145.105	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
109.67.119.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.168.133.63	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
81.82.200.255	147.237.8.46	Belgium	e.chinuch.idf.i	ET SCAN NMAP -sS window 1024	1
223.95.76.85	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
77.127.207.173	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.191.56.188	147.237.8.24	United States	e.lifestyle.idf	ET SCAN NMAP -sS window 1024	1
59.106.108.116	147.237.77.216	Japan	dover.idf.il	Tehila - Perl LWP with fake user agent	1
50.204.188.142	147.237.8.46	United States	e.chinuch.idf.i	ET SCAN NMAP -f -sS	1
176.13.7.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
158.255.6.220	147.237.8.24	Russian Federation	e.lifestyle.idf	ET SCAN NMAP -sS window 1024	1
122.224.145.105	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
109.66.173.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.82.200.255	147.237.8.46	Belgium	e.chinuch.idf.i	ET SCAN NMAP -sS window 3072	1
223.105.1.114	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

01-12-2016-19:04:01 to 01-12-2016-20:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.231.23	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	45
40.77.167.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
185.32.179.136	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
185.32.179.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	30
37.26.148.180	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	29
185.32.179.136	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	24
66.154.222.11	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
66.154.222.11	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
66.249.64.250	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
80.246.139.193	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
80.246.139.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
80.246.139.193	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
79.181.0.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.139.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
80.246.139.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
80.246.139.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
46.19.85.195	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.152.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.180.107.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.66.189.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.147.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
50.18.94.121	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.132	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.80	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
37.26.147.192	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.20.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.213.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.7.3	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.42	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.86.245	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.132.70.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.142.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.102.213.176	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
41.131.82.71	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.177.158.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.159.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.125.142.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.229.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
142.160.131.90	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.22.129.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.192.54	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	6
82.81.34.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.159.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.62.171	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
80.179.114.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.132	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

01-12-2016-19:04:01 to 01-12-2016-20:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.139.172.131	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 89.139.172.131	Block	189
87.69.146.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	89
46.19.85.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
87.69.146.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	27
176.13.18.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	18
109.67.235.42	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
109.186.49.58	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	9
31.154.253.217	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 31.154.253.217	Block	7
46.117.162.127	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	7
37.26.149.137	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.26.149.137	Block	6
89.139.135.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
212.76.122.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
80.74.100.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
79.176.188.52	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	3
37.26.148.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.12.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.149.137	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	2
2.54.155.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
80.246.136.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.233.64.190	Romania	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.34	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	1
149.78.185.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.117.252.172	Romania	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
2.54.55.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.69.165.52	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.78.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1233-he/atal.aspx	Block	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
46.117.171.168	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
176.13.14.234	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 176.13.14.234 (Unknown SSL Session)	None	1
84.108.123.225	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.123.225	Block	1
37.142.216.129	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8	Block	1
109.253.197.211	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl80.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2027-he/cogat.aspx	Block	1
217.132.159.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.30.124	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
87.69.53.108	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
185.32.179.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.74.100.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.196	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
149.88.140.141	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	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
79.117.252.172	Romania	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
2.54.135.53	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.69.210.224	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
46.120.24.238	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1

01-12-2016-19:04:01 to 01-12-2016-20:04:01