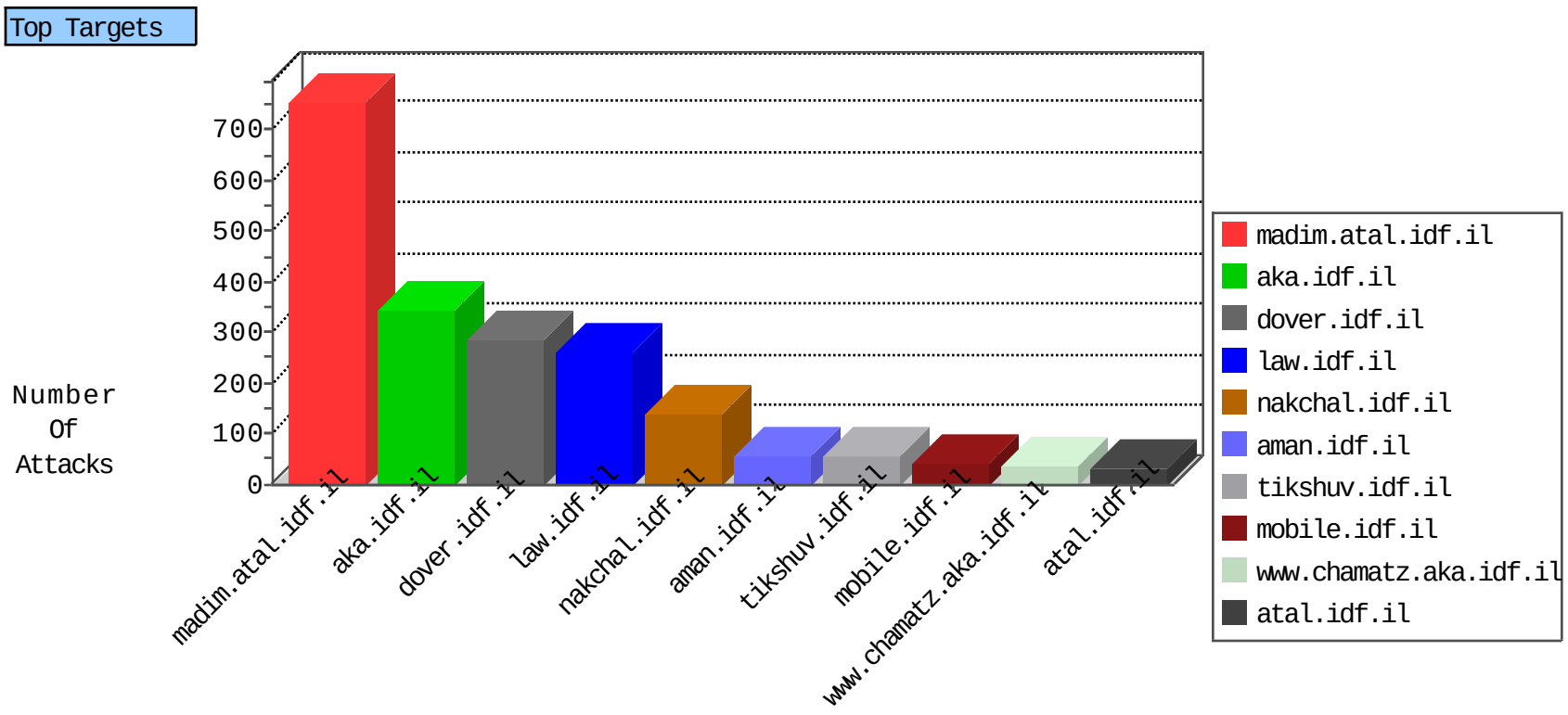
01-26-2016-18:04:04 to 01-26-2016-19:04:04

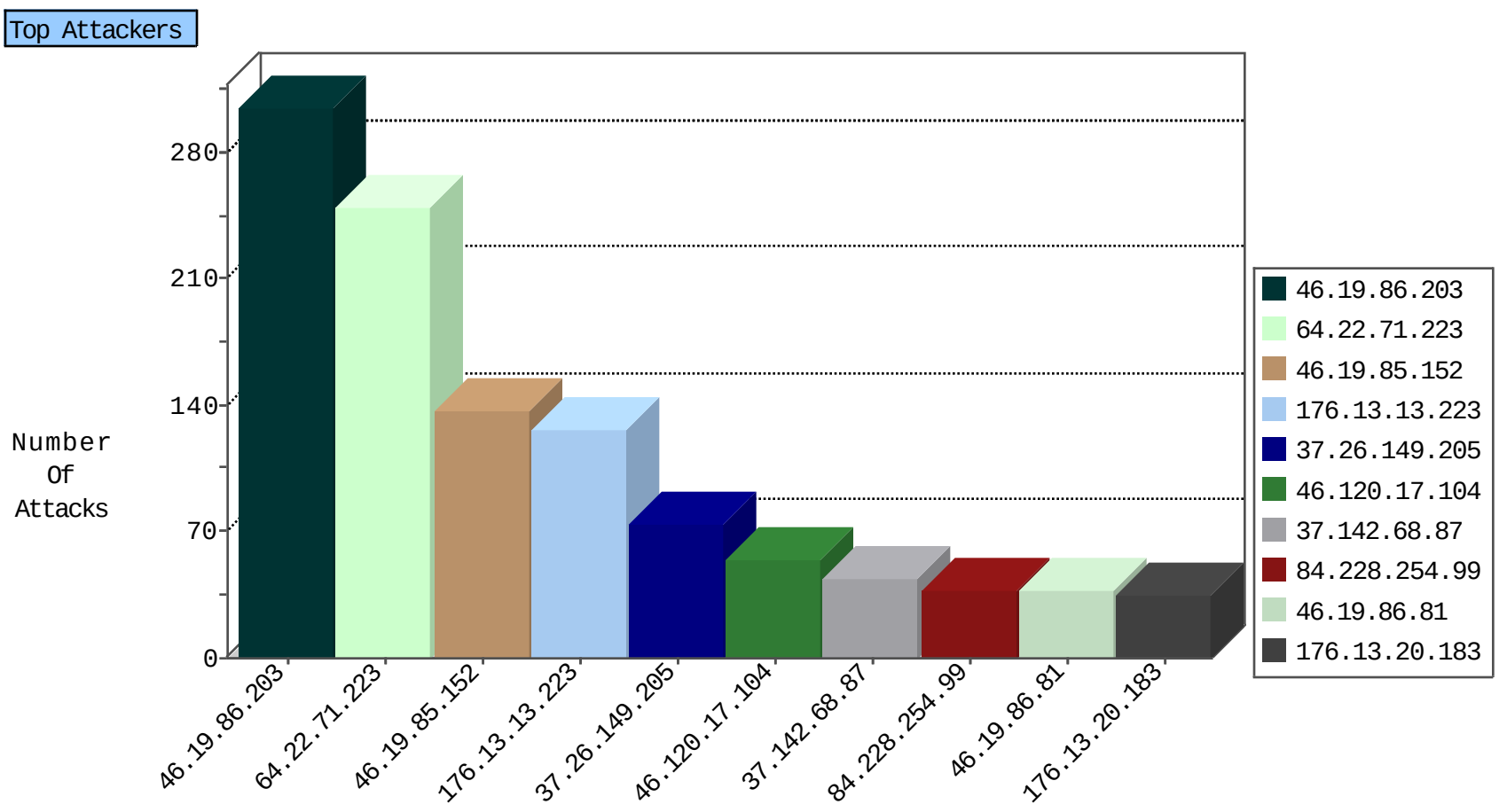
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-26-2016-18:04:04 to 01-26-2016-19:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.6.68	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
71.6.158.166	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
142.54.160.211	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1

01-26-2016-18:04:04 to 01-26-2016-19:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.173.50.36	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
198.50.134.71	Canada	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

01-26-2016-18:04:04 to 01-26-2016-19:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.152	147.237.76.31	Israel	nakchal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	101
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.159	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.6.161.154	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.1.229	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
147.236.232.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.254.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
114.112.90.54	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
109.66.175.132	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
85.250.88.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.116.217	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.142.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.252.193.52	147.237.76.197	Turkey	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
176.228.48.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
173.255.112.188	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.190.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
114.112.90.54	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.215.121	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.211.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.14.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.183.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.107.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.197.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-26-2016-18:04:04 to 01-26-2016-19:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
64.22.71.223	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	150
64.22.71.223	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	100
46.120.17.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.85.99	Israel	147.237.77.233	atal.idf.il	drop	SAM rule	drop	21
80.215.224.14	France	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	20
46.19.85.152	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	17
176.67.58.191	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	15
85.64.110.133	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	13
46.19.85.153	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
84.228.254.99	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
84.228.254.99	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
84.228.169.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.228.254.99	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.152	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Urgent Data Enforcement	TCP segment with urgent pointer (no data). Urgent data indication was stripped. Please refer to sk36869.	drop	6
79.183.108.59	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.64.80.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.9.46	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
80.246.133.165	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
2.52.50.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.247.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.168.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.50.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.247.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.121.123.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.33.8	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
94.230.84.54	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.152	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.52.50.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
95.86.88.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.29.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.179.200.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.152	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Urgent Data Enforcement	TCP segment with urgent pointer (no data). Urgent data indication was stripped. Please refer to sk36869.	alert	6
79.183.108.59	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	6
84.228.254.99	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.5.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.50.153	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	5
2.52.50.153	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.86.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.187.231	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
94.230.86.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
85.130.250.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.228.254.99	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence		monitor	5

01-26-2016-18:04:04 to 01-26-2016-19:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	166
46.19.86.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
176.13.13.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	105
37.26.149.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
37.142.68.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
176.13.20.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
46.19.86.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	29
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	28
46.19.86.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
176.13.13.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	20
176.13.16.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
37.142.68.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
85.64.110.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
50.87.144.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/english/&quot	Block	6
185.32.179.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.86.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.52.178.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
212.34.12.134	Jordan	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 212.34.12.134	Block	5
212.34.12.134	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 212.34.12.134	Block	5
212.34.12.134	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 212.34.12.134	Block	5
213.57.225.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
79.182.56.153	Israel	147.237.76.42	refuah.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.13.3.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.182.9.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.136.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
197.165.247.42	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
84.95.2.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
197.165.247.42	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	3
2.54.5.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.67.61.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.94.190.15	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	2
95.86.103.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1440-he/atal.aspx&sa=u&ved=0ahukewilqp-t7cfkahxffw8khu4hbxmqfgghmaa&sig2=ym6nbw_cerqbhxinqeppmw&usg=afqjcnhrfu5afztittzgctqi2phjrxnx2g	Block	2
37.26.147.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.139.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.20.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.62	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	2
109.64.163.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.18.84	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
79.176.10.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
31.168.193.122	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
84.111.66.32	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.246.133.165	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
213.57.214.34	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.34.12.134	Jordan	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
46.19.85.150	Israel	147.237.0.19	madim.atal.idf.i	Multiple Untraceable SSL Sessions from 46.19.85.150 (Unknown SSL Session)	None	1
79.179.56.171	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.228.183	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/shared/usercontrols/headerupper/	Block	1
192.115.88.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-26-2016-18:04:04 to 01-26-2016-19:04:04